kaspersky

Kaspersky Secure Mail Gateway

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 2.0.0.6478

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 25.12.2021

Обозначение документа: 643.46856491.00085-06 90 01

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

О "Лаборатории Касперского": https://www.kaspersky.ru/about/company

kaspersky

Содержание

kaspersky

Об этом руководстве

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия «Kaspersky Secure Mail Gateway» (далее по тексту – Kaspersky Secure Mail Gateway, программа).

Подготовительные процедуры изложены в разделах «Установка и первоначальная настройка программы», «Подготовка программы к работе» и «Процедура приемки» и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе «Требования» приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка и администрирование Kaspersky Secure Mail Gateway, а также поддержка организаций, использующих Kaspersky Secure Mail Gateway.

В этом разделе

В этом руководстве

В справку включены следующие разделы:

Источники информации о программе (на стр. 16)

Этот раздел содержит описание источников информации о программе.

Kaspersky Secure Mail Gateway (см. стр. 18)

Этот раздел содержит краткий обзор и функциональные возможности решения Kaspersky Secure Mail Gateway. Из раздела вы узнаете о режимах работы Kaspersky Secure Mail Gateway, аппаратных и программных требованиях.

Интерфейс Kaspersky Secure Mail Gateway (см. стр. 82)

Этот раздел содержит описание интерфейса программы.

Лицензирование программы (см. стр. 23)

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

Состояние защиты почтового сервера (см. стр. 84)

Этот раздел содержит информацию о том, как проверить уровень защиты почтового сервера и наличие проблем в защите.

Участие в Kaspersky Security Network (см. стр. 84)

Этот раздел содержит информацию об участии в Kaspersky Security Network.

Развертывание образа виртуальной машины программы в гипервизоре VMware™ESXi™ (см. стр. 48)

Этот раздел содержит пошаговые инструкции по развертыванию образа виртуальной машины программы в гипервизоре VMware ESXi.

Развертывание образа виртуальной машины программы в гипервизоре Microsoft® Hyper-V® (см. стр. 56)

Этот раздел содержит информацию о развертывании образа виртуальной машины программы в гипервизоре Microsoft Hyper-V.

Развертывание образа виртуальной машины программы в гипервизоре KVM (см. стр. 65)

Этот раздел содержит информацию о развертывании образа виртуальной машины программы в гипервизоре KVM.

Первоначальная настройка программы (см. стр. 67)

Этот раздел содержит пошаговые инструкции по первоначальной настройке Kaspersky Secure Mail Gateway, которую нужно выполнить после развертывания образа виртуальной машины Kaspersky Secure Mail Gateway.

Начало работы с программой (см. стр. 83)

Этот раздел содержит информацию о начале работы в веб-интерфейсе программы, в меню администратора программы и в режиме Technical Support Mode.

Настройка параметров MTA (см. стр. 278)

Этот раздел содержит информацию о настройке основных параметров MTA.

Мониторинг Kaspersky Secure Mail Gateway (см. стр. 92)

Этот раздел содержит информацию о мониторинге почтового трафика, последних обнаруженных угроз и ресурсов системы.

Обновление баз Kaspersky Secure Mail Gateway (см. стр. 216)

Этот раздел содержит информацию об обновлении антивирусных баз, баз модулей Анти-Спам и Анти-Фишинг.

Обновление Kaspersky Secure Mail Gateway через веб-интерфейс (см. стр. 214)

Этот раздел содержит информацию об обновлении Kaspersky Secure Mail Gateway через веб-интерфейс.

Антивирусная защита сообщений (см. стр. 204)

Этот раздел содержит информацию об антивирусной защите сообщений и настройке ее параметров.

Защита сообщений от спама (см. стр. 206)

Этот раздел содержит информацию о защите сообщений от спама и настройке ее параметров.

Защита сообщений от фишинга (см. стр. 208)

Этот раздел содержит информацию о защите сообщений от фишинга и настройке ее параметров.

Контентная фильтрация сообщений (см. стр. 208)

Этот раздел содержит информацию о контентной фильтрации сообщений и настройке ее параметров.

Работа с правилами обработки сообщений (см. стр. 98)

Этот раздел содержит информацию о правилах обработки сообщений, настройке их параметров и настройке параметров Kaspersky Secure Mail Gateway для каждого правила обработки сообщений.

Соединение с LDAP-сервером (см. стр. 224)

Этот раздел содержит информацию о соединении Kaspersky Secure Mail Gateway с LDAP-сервером и о настройке параметров и фильтров соединения с LDAP-сервером.

Почтовые уведомления Kaspersky Secure Mail Gateway (см. стр. 262)

Этот раздел содержит информацию о почтовых уведомлениях Kaspersky Secure Mail Gateway и настройке их параметров.

Резервное хранилище (см. стр. 150)

Этот раздел содержит информацию о резервном хранилище и работе с ним.

DKIM-подпись к исходящим сообщениям (см. стр. 282)

Этот раздел содержит информацию о добавлении DKIM-подписи к исходящим сообщениям.

Работа с программой по протоколу SNMP (см. стр. 232)

Этот раздел содержит информацию о работе с программой по протоколу SNMP, а также о настройке ловушек событий, возникающих во время работы Kaspersky Secure Mail Gateway.

Журнал событий Kaspersky Secure Mail Gateway (см. стр. 163)

Этот раздел содержит информацию о журнале событий программы и настройке его параметров.

Отчеты о работе Kaspersky Secure Mail Gateway (см. стр. 183)

Этот раздел содержит информацию о том, как создавать и просматривать отчеты о работе Kaspersky Secure Mail Gateway.

Списки разрешенных и запрещенных адресов (см. стр. 123)

Этот раздел содержит информацию о списках разрешенных и запрещенных адресов электронной почты, которые можно создавать и редактировать в Kaspersky Secure Mail Gateway.

Использование протокола TLS в работе Kaspersky Secure Mail Gateway (см. стр. 286)

Этот раздел содержит информацию об использовании протокола TLS в работе Kaspersky Secure Mail Gateway и о настройке параметров использования протокола.

Очередь сообщений Kaspersky Secure Mail Gateway (см. стр. 176)

Этот раздел содержит информацию об очередях сообщений Kaspersky Secure Mail Gateway.

Журнал трассировки Kaspersky Secure Mail Gateway (см. стр. 328)

Этот раздел содержит информацию о журнале трассировки Kaspersky Secure Mail Gateway.

Проверка целостности файлов Kaspersky Secure Mail Gateway (см. стр. 136)

Этот раздел содержит информацию о проверке целостности файлов Kaspersky Secure Mail Gateway.

Антивирусная проверка модулем kavscanner (см. стр. 317)

Этот раздел содержит информацию об антивирусной проверке модулем kavscanner.

Обращение в Службу технической поддержки (см. стр. 327)

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

Информация о стороннем коде (см. стр. 337)

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках (см. стр. 338)

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком "Пример".

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком "стрелка".
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

kaspersky

Источники информации о программе

Этот раздел содержит описание источников информации о программе.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В этом разделе

Источники информации для самостоятельного поиска

Вы можете использовать следующие источники для самостоятельного поиска информации о Kaspersky Secure Mail Gateway:

- страница Kaspersky Secure Mail Gateway на веб-сайте "Лаборатории Касперского";
- страница Kaspersky Secure Mail Gateway на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского" (см. раздел "Обращение в Службу технической поддержки" на стр. 327).

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница Kaspersky Secure Mail Gateway на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Secure Mail Gateway (http://www.kaspersky.ru/business-security/mail-security-appliance) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Secure Mail Gateway содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница Kaspersky Secure Mail Gateway в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Secure Mail Gateway в Базе знаний (https://support.kaspersky.ru/ksmg) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Secure Mail Gateway, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка Kaspersky Secure Mail Gateway (справка веб-интерфейса)

С помощью веб-интерфейса вы можете управлять Kaspersky Secure Mail Gateway через браузер. Справка содержит информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя через веб-интерфейс Kaspersky Secure Mail Gateway (далее также "веб-интерфейс").

Документация

В комплект поставки Kaspersky Secure Mail Gateway включен настоящий документ "Kaspersky Secure Mail Gateway. Подготовительные процедуры и руководство по эксплуатации", с помощью которого вы можете установить программу и произвести настройку параметров программы.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе (https://community.kaspersky.com).

В сообществе вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

О Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway представляет собой средство антивирусной защиты типа "Б" четвертого класса защиты и предназначено для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используется Kaspersky Secure Mail Gateway, являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и / или съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В Kaspersky Secure Mail Gateway реализованы следующие функции безопасности:

- Разграничение доступа к управлению ОО
- Управление работой ОО
- Управление параметрами ОО
- Управление установкой обновлений (актуализации) БД ПКВ ОО
- Аудит безопасности ОО
- Выполнение проверок объектов воздействия
- Обработка объектов воздействия
- Сигнализация ОО
- Выполнение проверок сообщений электронной почты
- Идентификация и аутентификация
- Контроль целостности компонентов ОО

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования

Аппаратные требования к конфигурации виртуальной машины для развертывания ISO-образа

- 8 ядер процессора;
- 16 ГБ оперативной памяти;
- 200 ГБ дискового пространства.

Программные требования к компьютерам локальной сети организации (для аутентификации с помощью технологии SSO в веб-интерфейсе программы)

- Windows® 8.1.
- Windows 10 (1809, 20H2, 21H2).
- Windows 11 (21H2).

Программные требования к гипервизору для развертывания виртуальной машины

- VMware ESXi 6.7 Update 3b.
- VMware ESXi 7.0 Update 2d.
- Microsoft Hyper-V Server 2016 (только Generation 1).
- Microsoft Hyper-V Server 2019.
- KVM, запущенный на QEMU 2.12 на базе CentOS 7.

Программные требования для настройки интеграции с LDAP-сервером

- Windows Server® 2012 R2 Standard.
- Windows Server 2016 Standard.
- Windows Server 2019 Standard.
- Windows Server 2022 Standard.

Программные требования для работы с Kaspersky Secure Mail Gateway через веб-интерфейс

Для работы веб-интерфейса на компьютере должен быть установлен один из следующих браузеров:

- Mozilla™ Firefox™ версии 94.
- Google Chrome™ версии 96.
- Microsoft Edge версии 96.

Приведенные системные требования гарантируют пиковую пропускную способность Kaspersky Secure Mail Gateway 10 сообщений/сек. при среднем размере сообщения 300 КБ. Фактическая производительность программы зависит от модели процессора и его тактовой частоты. Для увеличения пропускной способности рекомендуется увеличить ресурсы виртуальной машины или развернуть несколько образов виртуальных машин, распределив поток сообщений электронной почты между ними, создав соответствующую запись на DNS-сервере, или с помощью служб балансировки сетевой нагрузки.

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

В Kaspersky Secure Mail Gateway предусмотрены следующие учетные записи:

- Учетная запись администратора виртуальной машины Kaspersky Secure Mail Gateway (далее также "администратор сервера", "администратор виртуальной машины") для управления сервером.

  Учетная запись администратора сервера служит для управления сервером с виртуальной машиной программы. Под этой учетной записью вы можете выключить или перезагрузить сервер.

  Учетная запись администратора сервера имеет доступ к данным на этом сервере. Пароль учетной записи администратора для работы в консоли управления сервером должен быть надежным. Администратору необходимо обеспечить безопасность сервера самостоятельно. Администратор несет ответственность за доступ к данным, хранящимся на сервере.

- Учетная запись суперпользователя программы Administrator.

  Учетная запись администратора веб-интерфейса программы Administrator создается при установке программы и обладает всем набором прав на управление программой. Эта учетная запись предназначена для сотрудников вашей организации, в чьи обязанности входит управление Kaspersky Secure Mail Gateway через веб-интерфейс программы.

- Учетные записи администраторов веб-интерфейса.

  Суперпользователь Administrator может назначить роль с ограниченным набором прав на управление программой другим сотрудникам, например, офицеру безопасности.

  Таким пользователям, которым назначена хотя бы одна роль (см. раздел "Назначение роли" на стр. 148), доступен просмотр веб-интерфейса в режиме администратора. В меню отображаются те разделы, на которые у администратора есть права.

- Учетные записи пользователей.

  Режим пользователя доступен всем пользователям домена, если настроена интеграция с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 224). Для просмотра веб-интерфейса в режиме пользователя требуется войти в программу (см. раздел "Подключение к веб-интерфейсу программы" на стр. 83), используя доменную учетную запись. В меню отображаются разделы с персональным Хранилищем и персональными списками разрешенных и запрещенных адресов. В этих разделах доступна информация только о сообщениях и адресах текущего пользователя.

kaspersky

Режимы работы Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway может работать в обычном режиме, в режиме ограниченного трафика или в сертифицированном режиме.

В обычном режиме Kaspersky Secure Mail Gateway разрешен доступ в интернет и соединение со следующими серверами, расположенными за пределами IT-инфраструктуры вашей организации:

- Серверами обновлений баз KSN.
- DNS-серверами.
- Серверами обновлений баз Kaspersky Secure Mail Gateway.

В режиме ограниченного трафика Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации.

В режиме ограниченного трафика параметры компонентов Kaspersky Secure Mail Gateway, требующих доступ в интернет, по умолчанию принимают следующие значения:

- Использование KSN отключено.
- SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений отключены, соединение с DNS-серверами запрещено.
- Функция Enforced Anti-Spam Updates отключена в параметрах модуля Анти-Спам.
- В качестве источника обновлений баз Kaspersky Secure Mail Gateway используется Kaspersky Security Center или локальный источник обновлений баз Kaspersky Secure Mail Gateway.

В сертифицированном режиме Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации.

Вы можете выбрать сертифицированный режим работы Kaspersky Secure Mail Gateway при развертывании образа виртуальной машины Kaspersky Secure Mail Gateway.

kaspersky

Лицензирование приложения

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием приложения Kaspersky Secure Mail Gateway.

В сертифицированной версии Kaspersky Secure Mail Gateway допускается только активация файлом ключа. Иные способы активации ведут к выходу из безопасного состояния программы.

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки Kaspersky Secure Mail Gateway.
- Прочитав документ license.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

kaspersky

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в программу, применив *файл ключа*.

Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Для Kaspersky Secure Mail Gateway используются ключи следующих типов:

- *Полнофункциональный ключ*. При добавлении ключа программа работает в режиме полной функциональности, осуществляются проверки на спам, фишинг, вирусы и другие программы, представляющие угрозу, контентная фильтрация, проверка подлинности отправителей сообщений и проверка сообщений в Kaspersky Anti Targeted Attack Platform.
- *Ключ для антивирусной защиты*. При добавлении ключа программа производит поиск вирусов и других программ, представляющих угрозу, контентную фильтрацию, проверку подлинности отправителей сообщений и проверку сообщений в Kaspersky Anti Targeted Attack Platform. Программа не производит проверку на спам. Статус, присвоенный программой сообщению при проверке, содержит информацию об ограниченной функциональности.
- *Ключ для защиты от спама и фишинга*. При добавлении ключа программа производит проверку на спам и фишинг, контентную фильтрацию, проверку подлинности отправителей сообщений и проверку сообщений в Kaspersky Anti Targeted Attack Platform. Программа не производит поиск вирусов и других программ, представляющих угрозу. Статус, присвоенный программой сообщению при проверке, содержит информацию об ограниченной функциональности.

Антивирусные базы и базы Анти-Спама обновляются независимо от типа ключа.

kaspersky

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Secure Mail Gateway или после заказа пробной версии Kaspersky Secure Mail Gateway.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

О подписке

Подписка на Kaspersky Secure Mail Gateway – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств).

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Secure Mail Gateway после окончания ограниченной подписки ее требуется продлить. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Чтобы использовать Kaspersky Secure Mail Gateway по подписке, требуется применить код активации. После применения кода активации устанавливается ключ, определяющий лицензию на использование программы по подписке.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Secure Mail Gateway.

О предоставлении данных

Для работы программы используются данные, на отправку и обработку которых требуется согласие администратора Kaspersky Secure Mail Gateway.

Вы можете ознакомиться с перечнем данных и условиями их использования, а также дать согласие на обработку данных в следующих соглашениях между вашей организацией и "Лабораторией Касперского":

- В Лицензионном соглашении.

  Согласно условиям принятого Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять "Лаборатории Касперского" информацию, которая требуется для повышения

уровня защиты почтового сервера. Эта информация перечислена в Лицензионном соглашении в пункте Условия обработки данных:

- идентификатор программы;
- уникальный идентификатор активации текущего лицензионного кода активации;
- идентификатор установки программы;
- название и версия программы.

- В Политике конфиденциальности.
- В Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network.

  При участии в Kaspersky Security Network и при отправке KSN-статистики в "Лабораторию Касперского" может передаваться информация, полученная в результате работы программы. Перечень передаваемых данных указан в Положении о Kaspersky Security Network и в Дополнительном Положении о Kaspersky Security Network.

Защита данных

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Оперативная память Kaspersky Secure Mail Gateway может содержать любые обрабатываемые данные пользователей программы. Администратору Kaspersky Secure Mail Gateway необходимо обеспечить безопасность этих данных самостоятельно.

По умолчанию доступ к персональным данным пользователей имеют только учетная запись суперпользователя операционных систем root, учетная запись администратора Kaspersky Secure Mail Gateway Локальный администратор, а также системные учетные записи kluser, postfix, opendkim и nginx, от имени которых работают компоненты программы. Возможность ограничить права администраторов и других пользователей операционных систем, на которые установлена программа, средствами самой программы не предусмотрена. Доступ к месту хранения данных ограничен средствами файловой системы. Администратору рекомендуется контролировать доступ к персональным данным других пользователей любыми системными средствами на его усмотрение.

Передача данных между узлами кластера осуществляются по зашифрованному каналу (по протоколу HTTPS с использованием авторизации пользователей с помощью сертификата безопасности). Передача данных в веб-интерфейс осуществляются по зашифрованному каналу по протоколу HTTPS. Пользователи веб-интерфейса проходят процедуру аутентификации, а Локальный администратор – авторизацию по паролю.

Доставка электронной почты поддерживает шифрование SMTPS.

Работа с программой из консоли управления сервера, на котором установлена программа, под учетной записью суперпользователя позволяет управлять параметрами дампа. Дамп формируется при сбоях программы и может понадобиться при анализе причины сбоя. В дамп могут попасть любые данные, включая фрагменты анализируемых файлов. По умолчанию формирование дампа в Kaspersky Secure Mail Gateway отключено.

Доступ к этим данным может быть осуществлен из консоли управления сервера, на котором установлена программа, под учетной записью суперпользователя.

При передаче диагностической информации в Службу технической поддержки "Лаборатории Касперского" администратору Kaspersky Secure Mail Gateway необходимо обеспечить безопасность дампов и файлов трассировки самостоятельно.

Администратор Kaspersky Secure Mail Gateway несет ответственность за доступ к данной информации.

Состав данных, которые могут храниться в программе

Для ознакомления с полным перечнем данных пользователей, которые могут храниться в Kaspersky Secure Mail Gateway, см. таблицу ниже.

Таблица 2. Данные пользователей, которые могут храниться в Kaspersky Secure Mail

Gateway

Тип данных	Где используются данные	Место хранения	Срок хранения	Доступ
Основная функциональность программы				
• Имена учетных записей администратора и пользователей программы. • Права доступа учетных записей программы. • Хеш пароля Локального администратора. • Имя учетной записи и пароль подключения программы к прокси-серверу. • Keytab-файлы для подключения к LDAP-серверу. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. • Комментарии.	Конфигурация программы	/var/opt/kaspersky	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр параметров программы.
• Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты. • Адреса электронной почты отправителей и получателей сообщений. • IP-адреса пользователей и почтовых серверов. • Комментарии.	Правила обработки сообщений	/var/opt/kaspersky	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр правил обработки сообщений.
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. Информация о LDAP-атрибутах пользователей: • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.	Статистика работы программы	/var/opt/kaspersky	Бессрочно.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр отчетов и раздела Мониторинг.

Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Имена почтовых вложений. • Тема сообщения. Информация о LDAP-атрибутах пользователей: • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.	Журнал событий обработки сообщений	/var/opt/kaspersky	Согласно параметрам, заданным пользователем программы. По умолчанию устанавливается срок хранения 3 дня или максимальный размер журнала 1 ГБ. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр журнала событий обработки сообщений.
		/var/log/ksmg-messages	Бессрочно. При достижении объема 23 ГБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.
		/var/log/ksmg-important	Бессрочно. При достижении объема 500 МБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.

• Имя учетной записи пользователя, инициировавшего событие. • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений.	Журнал системных событий	/var/opt/kaspersky	Согласно параметрам, заданным пользователем программы. По умолчанию хранится 100 тысяч записей. При достижении этого ограничения более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр журнала системных событий.
		/var/log/ksmg-messages	Бессрочно. При достижении объема 23 ГБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.
		/var/log/ksmg-important	Бессрочно. При достижении объема 500 МБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.

Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений. Данные об обновлениях программы: • IP-адреса, используемые для скачивания обновлений. • IP-адреса источников обновлений. • Информация о скачиваемых файлах и скорости скачивания. Информация об учетных записях пользователей: • Имена учетных записей администраторов и пользователей веб-интерфейса программы. • Имена учетных записей пользователей в LDAP и другие LDAP-атрибуты.	Файлы трассировки	/var/log/kaspersky	Бессрочно. При достижении объема 150 МБ для каждого потока трассировки более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации и при записи событий в журнал. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.
		/var/log/kaspersky/extra	Бессрочно. При достижении объема 400 МБ для каждого потока трассировки более старые записи удаляются.	
		/var/log/ksmg-traces	Бессрочно. При достижении объема 23 ГБ для каждого потока трассировки более старые записи удаляются.	
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений.	Хранилище	/var/opt/kaspersky	Бессрочно. При достижении объема 7 ГБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Службы postfix и opendkim имеют доступ к сообщениям во время их доставки из Хранилища. • Пользователи веб-интерфейса программы, имеющие права на просмотр Хранилища.

Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений.	Анти-Спам карантин	/var/opt/kaspersky	Бессрочно. При достижении объема 1 ГБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр Анти-Спам карантина.
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений. • URL-адреса, содержащиеся в сообщении.	KATA-карантин	/var/opt/kaspersky	Бессрочно. При достижении объема 1 ГБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр KATA-карантина.
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений.	Временные файлы	• /tmp/ksmgtmp • /tmp/klms_filter	До перезагрузки программы.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Службы postfix и opendkim имеют доступ к обработанным сообщениям во время их доставки.
Интеграция с Active Directory				

• Адрес электронной почты пользователя. • DN пользователя. • CN пользователя. • sAMAccountName. • UPN-суффикс. • objectSID.	• Правила обработки сообщений. • Аутентификация с помощью технологии единого входа. • Автозаполнение учетных записей при работе с ролями и правами пользователей, а также при настройке правил обработки сообщений.	/var/opt/kaspersky/ksmg/ldap/cache.dbm	Бессрочно. Данные регулярно обновляются. При отключении интеграции программы с Active Directory данные удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на автозаполнение учетных записей.
Интеграция с программой Kaspersky Anti Targeted Attack Platform (KATA)				
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения. • Имена и тела почтовых вложений. • URL-адреса, содержащиеся в сообщении.	Отправка объектов для проверки на сервере KATA	Данные не сохраняются.	Данные не сохраняются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке.
Функциональность встроенного почтового сервера				

• Сертификаты для установки TLS-соединений. • Файлы приватных ключей сертификатов[1]. • Приватные ключи для DKIM-подписей. • Адреса электронной почты пользователей. • IP-адреса и доменные имена почтовых серверов.	Параметры встроенного почтового сервера	/etc/postfix/ /var/opt/kaspersky/	Бессрочно. Данные удаляются при удалении соответствующих параметров в веб-интерфейсе программы. Файлы сертификатов могут быть перезаписаны при замене сертификата.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Службы postfix и opendkim имеют доступ к месту хранения информации, а также к данным при их обработке. • Пользователи веб-интерфейса программы, имеющие права на просмотр параметров встроенного почтового сервера, имеют доступ к данным, кроме приватных ключей.
Информация из электронной почты: • IP-адреса пользователей и почтовых серверов. • Адреса электронной почты отправителей и получателей сообщений. • Доменные имена почтовых серверов. • Данные о TLS-шифровании.	Журнал событий встроенного почтового сервера	/var/log/maillog	Бессрочно. При достижении объема 100 МБ более старые записи удаляются.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при получении диагностической информации. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Службы postfix и opendkim имеют доступ к данным при записи событий в журнал. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.

[1] Доступ к файлам возможен только по протоколу SSH после загрузки открытого ключа SSH через веб-интерфейс программы.

Информация из электронной почты: • Адреса электронной почты отправителей и получателей сообщений. • Тема сообщения. • Тело сообщения. • Служебные заголовки сообщения.	Очереди сообщений встроенного почтового сервера	/var/spool/postfix	Бессрочно. Сообщения удаляются по мере их доставки получателям.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при управлении очередями сообщений встроенного почтового сервера. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Служба postfix имеет доступ к данным при их обработке. • Пользователи веб-интерфейса программы, имеющие права на просмотр очередей сообщений.
Подключение по протоколу SSH: • IP-адрес пользователя. • Имя учетной записи пользователя. • Отпечаток ключа SSH. Подключение через веб-интерфейс: • IP-адрес пользователя. • Имя учетной записи пользователя.	Журнал событий авторизации	/var/log/secure	Не более 5 недель. Выполняется еженедельная ротация файлов.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при их обработке. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на получение диагностической информации.
Открытые ключи SSH администраторов программы.	Параметры встроенного SSH-сервера	/etc/ssh/authorized_keys	Бессрочно. Данные удаляются при удалении соответствующих параметров в веб-интерфейсе программы.	• Пользователь root имеет доступ к месту хранения информации. • Пользователь kluser имеет доступ к месту хранения информации, а также доступ к данным при управлении параметрами встроенного SSH-сервера. • Служба nginx имеет доступ к данным при их передаче между узлами, а также при передаче в веб-интерфейс. • Пользователи веб-интерфейса программы, имеющие права на просмотр параметров встроенного SSH-сервера.

Состав данных, передаваемых в службу Kaspersky Security Network

Данные передаются на серверы KSN в зашифрованном виде. По умолчанию доступ к данным имеют специалисты "Лаборатории Касперского", учетная запись суперпользователя операционных систем root, а также системная учетная запись kluser, от имени которой работают компоненты программы.

Для ознакомления с полным перечнем данных пользователей, передаваемых в службу KSN, см. таблицу ниже.

Указанные данные передаются только в случае согласия на участие в Kaspersky Security Network.

Таблица 3. Данные, передаваемые в службу Kaspersky Security Network

Тип данных	Где используются данные	Место хранения	Срок хранения
• Контрольные суммы (MD5, SHA2-256) проверяемого объекта; • URL-адрес, репутация которого запрашивается; • идентификатор протокола соединения и номер используемого порта; • идентификатор антивирусных баз и идентификатор записи в антивирусных базах, которые использовались для проверки объекта; • информация о сертификате подписанного файла (отпечаток сертификата и контрольная сумма (SHA256) публичного ключа сертификата); • идентификатор и полная версия установленного ПО; • идентификатор службы KSN, к которой обращается ПО; • дата и время отправки объекта на проверку; • идентификатор компонента ПО; • идентификатор сценария, в рамках которого объект отправлен на проверку.	Отправка KSN-запросов	KSN-серверы	Бессрочно. Максимальное количество хранимых записей составляет 360 тысяч. При достижении этого ограничения удаляются записи, к которым дольше всего не было обращений.

Тип данных	Где используются данные	Место хранения	Срок хранения
• Информация об операционной системе, установленной на компьютере (тип; версия; разрядность). • Информация об установленной программе и компьютере (уникальный идентификатор компьютера, на котором установлена программа; уникальный идентификатор установки программы на компьютере; название, локализация, идентификатор и полная версия установленной программы; дата и время установки ПО). • Информация о проверяемых объектах (идентификатор баз программы и идентификатор записи в базах программы; название обнаруженной угрозы согласно классификации АО «Лаборатория Касперского»; контрольная сумма (MD5, SHA256); размер, название и тип проверяемого объекта; полный путь к проверяемому объекту; дата и время проверки объекта; IP-адрес пользователя; результат проверки файлов и URL-адресов; метаданные проверяемых объектов; проверяемый URL-адрес; заголовок Referrer; контрольная сумма проверяемого URL-адреса; контрольная сумма и размер пакера и контейнера проверяемого объекта; дата и время последнего установленного обновления баз; флаг, поясняющий, является ли обнаружение отладочным). • Информация о проверяемых сообщениях электронной почты (идентификатор сообщения; время получения сообщения; цель атаки (название организации, веб-сайт); весовой уровень атаки; значение уровня доверия; IP-адрес отправителя из SMTP-сессии; информация из заголовков сообщения; IP-адреса промежуточных почтовых агентов; данные из SMTP-сессии; использованные методы обнаружения; фрагмент DKIM-подписи сообщения; информация о результатах проверки подлинности отправителя сообщения; информация о подключениях к DNS-серверу; информация из сообщения для обнаружения спама; размер сообщения в байтах; размер вложения в байтах; контрольная сумма и тип вложения; размер темы письма в байтах; имя кодировки письма; информация о том, что сообщение находилось в Анти-Спам карантине; информация об html-разметке сообщения; контрольная сумма и размер MIME-партов). • Информация о работе компонента Updater (версия компонента Updater; статус завершения задачи обновления компонента Updater; тип и идентификатор ошибки при обновлении компонента Updater в случаае ее возникновения; код завершения задачи обновления компонента Updater; количество аварийных завершений работы компонента Updater при выполнении задач обновления за время работы этого компонента). • Информация об ошибках, возникших в работе компонентов ПО (информация о компонентах ПО, в работе которых произошла ошибка; идентификатор типа ошибки; фрагменты отчетов о работе компонентов). • Информация о версии пакета статистики, дате и времени начала получения статистики, дате и времени окончания получения статистики. • Информация о лицензии, по которой используется ПО (идентификатор лицензии, идентификатор партнера, у которого приобретена лицензия, серийный номер лицензии, дата и время добавления лицензионного ключа, признак принятия Положения о KSN).	Отправка KSN-статистики	KSN-серверы	До отправки статистики в KSN. После отключения отправки KSN-статистики в параметрах программы данные удаляются при следующей попытке отправки.

При обновлении баз программы с серверов "Лаборатории Касперского" передается следующая информация:

- тип и версия программы;
- уникальный идентификатор действующего лицензионного ключа
- уникальный идентификатор установки программы
- идентификатор сессии обновления.

Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией

В Kaspersky Secure Mail Gateway предусмотрены различные режимы работы в зависимости от лицензии.

Без лицензии

В этом режиме Kaspersky Secure Mail Gateway работает с момента установки программы и запуска веб-интерфейса до тех пор, пока вы не добавите активный ключ.

В режиме **Без лицензии** Kaspersky Secure Mail Gateway не выполняет проверку сообщений электронной почты.

Пробная лицензия

В этом режиме Kaspersky Secure Mail Gateway выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа пробной лицензии, Kaspersky Secure Mail Gateway прекращает проверку сообщений электронной почты и обновление баз.

Для возобновления работы Kaspersky Secure Mail Gateway необходимо установить ключ коммерческой лицензии.

Коммерческая лицензия

В этом режиме Kaspersky Secure Mail Gateway выполняет проверку сообщений электронной почты и обновляет базы.

По истечении срока годности ключа коммерческой лицензии Kaspersky Secure Mail Gateway продолжает проверку сообщений электронной почты, но прекращает обновление баз.

Для возобновления обновления баз необходимо установить новый ключ коммерческой лицензии или продлить срок действия ключа коммерческой лицензии.

В Kaspersky Secure Mail Gateway предусмотрены ключи коммерческой лицензии следующих типов:

- *Полнофункциональный ключ*. При добавлении ключа программа работает в режиме полной функциональности, осуществляются проверки на спам, фишинг, вирусы и другие программы, представляющие угрозу.
- *Ключ для антивирусной защиты*. При добавлении ключа программа производит поиск вирусов и других программ, представляющих угрозу, не производит проверку на спам. Статус, присвоенный программой сообщению при проверке на спам, содержит информацию об ограниченной функциональности.

- *Ключ для защиты от спама и фишинга*. При добавлении ключа программа производит проверку на спам и фишинг, не производит поиск вирусов и других программ, представляющих угрозу. Статус, присвоенный программой сообщению при поиске вирусов и других программ, представляющих угрозу, содержит информацию об ограниченной функциональности.

Список запрещенных ключей

В ряде случаев ключ может быть занесен в список запрещенных ключей. Если это произошло, Kaspersky Secure Mail Gateway прекращает проверку сообщений электронной почты, но продолжает попытки обновления баз на случай, если ключ будет исключен из списка запрещенных ключей.

Как только ключ будет исключен из списка запрещенных ключей, Kaspersky Secure Mail Gateway возобновит проверку сообщений электронной почты в соответствии с действующей лицензией.

После отключения проверки сообщений электронной почты в Kaspersky Secure Mail Gateway продолжает работать почтовый агент MTA, соединение с LDAP-сервером, журнал событий, отчеты о работе Kaspersky Secure Mail Gateway, а также остается доступно управление всеми параметрами Kaspersky Secure Mail Gateway, кроме параметров защиты, через веб-интерфейс.

Добавление файла ключа

Рекомендуется активировать программу с помощью кода активации.

► *Чтобы добавить файл ключа, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. Нажмите на кнопку **Добавить лицензионный ключ**.

   Откроется окно **Добавление лицензионного ключа**.
3. В раскрывающемся списке **Тип лицензионного ключа** выберите **Файл ключа**.
4. В блоке **Файл лицензионного ключа** нажмите на кнопку **Обзор**.

   Откроется окно выбора файла.
5. Выберите файл ключа, который вы хотите добавить, и нажмите на кнопку **Open**.
6. Нажмите на кнопку **Активировать**.

Файл ключа будет добавлен, программа будет активирована. Вы можете проверить состояние лицензионного ключа (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 43) на узлах кластера.

kaspersky

Удаление ключа

Если вы удалите лицензионный ключ, вы не сможете использовать программу в режиме той функциональности, которую предусматривает ваша лицензия.

► *Чтобы удалить ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Лицензирование**.
2. Нажмите на кнопку **Удалить лицензионный ключ**.
3. В окне подтверждения нажмите на кнопку **ОК**.

Лицензионный ключ будет удален.

Мониторинг статуса лицензионного ключа

Чтобы отслеживать проблемы, связанные с лицензионным ключом, вы можете просматривать сводную информацию о состоянии лицензирования на всех узлах кластера на информационной панели **Лицензирование** в разделе **Узлы**.

Возможны следующие статусы лицензионного ключа:

- *Без ошибок* – добавлен действующий лицензионный ключ.
- *Предупреждения* – срок действия лицензионного ключа скоро истекает.

  Вы можете настроить, за сколько дней до истечения будет отображаться этот статус в параметрах лицензирования (см. раздел "Настройка предупреждений о скором истечении лицензионного ключа" на стр. 44).

- *Ошибки* – лицензионный ключ не добавлен или возникли ошибки лицензирования (например, истек срок действия ключа, ключ находится в списке запрещенных, предназначен для другой программы и т.д.).

В правой части информационной панели указано количество узлов кластера по каждому статусу.

► *Чтобы просмотреть детальную информацию о состоянии лицензионного ключа на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Лицензирование** перейдите в раздел **Параметры** → **Лицензирование** → **Статус лицензионного ключа**.

В верхней части раздела отображается блок параметров с информацией о добавленном лицензионном ключе:

- Состояние лицензионного ключа (например, *Активный лицензионный ключ* или *Недопустимый формат лицензионного ключа*).
- **Тип лицензии** – тип лицензии (пробная или коммерческая).

- **Уровень функциональности** – режим работы программы (см. раздел "Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией" на стр. 41).
- **Серийный номер** – уникальная последовательность из латинских букв и цифр.
- **Программа** – название программы, для которой предназначен лицензионный ключ.

В нижней части раздела отображается таблица узлов кластера с информацией о статусе лицензионного ключа на каждом узле:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Статус лицензионного ключа** – подробное описание статуса лицензионного ключа на узле кластера.
- **Серийный номер** – уникальная последовательность из латинских букв и цифр.
- **Дата истечения** – дата и время, когда текущая лицензия перестанет действовать и программа перестанет получать обновления баз (см. раздел "Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией" на стр. 41).

Таблица отображается при наличии у пользователя прав **Просматривать информацию об узлах** и/или **Создавать/изменять/удалять узлы**, а также **Просматривать параметры** и/или **Изменять параметры**.

Вы также можете просмотреть сведения о добавленном лицензионном ключе в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130).

Настройка предупреждений о скором истечении лицензионного ключа

Вы можете настроить предупреждения о скором истечении лицензионного ключа в веб-интерфейсе программы. Когда до истечения срока действия остается заданное количество дней, администратору отображается предупреждение в следующих разделах веб-интерфейса:

- в разделе **Узлы** на информационной панели **Лицензирование** (см. раздел "**Мониторинг статуса лицензионного ключа**" на стр. 43);
- в окне просмотра информации об узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130);
- в таблице о состоянии лицензионного ключа на узлах кластера (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 43) в разделе **Параметры** → **Лицензирование** → **Статус лицензионного ключа**.

► *Чтобы настроить предупреждения о скором истечении лицензионного ключа:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Лицензирование** → **Параметры лицензирования**.
2. В поле **Предупреждать о скором истечении лицензионного ключа (в днях)** укажите, за сколько дней до истечения срока действия лицензионного ключа вы хотите получать предупреждение в веб-интерфейсе программы.

Если вы хотите, чтобы предупреждения не отображались, установите значение 0.

Возможные значения – целые числа от 0 до 99. Значение по умолчанию – 30.

3. Нажмите на кнопку **Сохранить**.

Предупреждения о скором истечении лицензионного ключа будут настроены.

kaspersky

Установка и первоначальная настройка программы

Вы можете установить программу на физическом сервере или на виртуальной машине. Поддерживается развертывание виртуальной машины на следующих гипервизорах:

- VMware ESXi.

  Вы можете выполнять все действия по развертыванию виртуальной машины в следующих интерфейсах:

  - в веб-интерфейсе VMware vSphere™ (см. раздел "Развертывание виртуальной машины в веб-интерфейсе VMware vSphere" на стр. 52);
  - в консоли управления гипервизора VMware ESXi (см. раздел "Развертывание виртуальной машины в консоли управления гипервизора VMware ESXi" на стр. 48).

- Microsoft Hyper-V.

  Вы можете выполнять все действия по развертыванию виртуальной машины в следующих интерфейсах:

  - в интерфейсе программы Microsoft System Center Virtual Machine Manager (см. раздел "Развертывание виртуальной машины с помощью программы Microsoft SCVMM" на стр. 60) (далее также Microsoft SCVMM);
  - в консоли управления Microsoft Hyper-V Manager (см. раздел "Развертывание виртуальной машины в консоли управления гипервизора Microsoft Hyper-V Manager" на стр. 56).

- KVM.

Убедитесь, что версия гипервизора и аппаратные ресурсы, выделенные для виртуальной машины, удовлетворяют аппаратным и программным требованиям.

После развертывания виртуальной машины вы можете перейти к установке программы. Для этого вам потребуются следующие файлы:

- Дистрибутив (rpm-пакеты) программы.
- ISO-образ установочного диска операционной системы CentOS Linux® 7.

Дополнительные пакеты будут загружены автоматически из публичных репозиториев в сети Интернет в процессе установки.

kaspersky

В этом разделе

Подготовка и первоначальная настройка операционной системы

Для выполнения всех действий, описанных в этом разделе, учетная запись должна обладать правами суперпользователя.

Установка операционной системы

После подключения к развернутой виртуальной машине требуется выполнить установку операционной системы в минимальной конфигурации. Во время установки вам нужно провести разметку жесткого диска. При этом рекомендуется создать на жестком диске корневой раздел /, занимающий все дисковое пространство.

После завершения установки вы можете перейти к первоначальной настройке операционной системы.

Первоначальная настройка операционной системы

► *Выполните следующие действия для подготовки операционной системы к установке программы:*

1. Настройте на виртуальной машине сетевое подключение для доступа в интернет.

   Доступ в интернет потребуется для загрузки дополнительных пакетов.

2. Отключите SELinux. Для этого в конфигурационном файле /etc/sysconfig/selinux установите значение параметра `SELINUX=disabled`.

3. Перезагрузите операционную систему.

Операционная система готова к установке программы.

kaspersky

Подготовка ISO-образа

Для выполнения всех действий, описанных в этом разделе, учетная запись должна обладать правами суперпользователя.

► *Чтобы установить пакеты программы, выполните следующие действия:*

1. Скопируйте архив ksmg_2.0.0.6478_iso_build.tgz, содержащий дистрибутив программы, на виртуальную машину.
2. Подключитесь к виртуальной машине по протоколу SSH и распакуйте скопированный на предыдущем шаге архив.
3. Выполните следующую команду:

   ```
   sh /root/ksmg_2.0.0.6478/iso_build/build_iso.sh
   ```

Пакеты программы будут установлены. Подготовленный ISO-образ будет храниться в директории /root/ksmg_2.0.0.6478/iso_build/tmp/build/iso-inst.dir/ksmg-2.0.0-6478-inst.x86_64_mlg.iso.

Развертывание виртуальной машины в консоли управления гипервизора VMware ESXi

Развертывание образа виртуальной машины состоит из следующих этапов:

a. **Загрузка ISO-файла в виртуальное хранилище данных (см. раздел "Загрузка ISO-файла" на стр. 49)**

   ISO-файл Kaspersky Secure Mail Gateway содержит образ операционной системы с предустановленной программой и встроенным почтовым сервером.

b. **Создание виртуальной машины (см. раздел "Создание виртуальной машины в консоли управления гипервизора VMware ESXi" на стр. 49)**

   Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Secure Mail Gateway.

c. **Изменение параметров виртуальной машины (на стр. 51)**

   Если вы хотите подключить виртуальную машину к нескольким сегментам сети, вам нужно добавить дополнительный сетевой адаптер для каждого сегмента. Если этого не требуется, вы можете пропустить этот этап.

d. **Подключение к виртуальной машине и запуск мастера первоначальной настройки программы (см. раздел "Подключение к виртуальной машине и запуск мастера первоначальной настройки" на стр. 51)**

   Перед началом работы с Kaspersky Secure Mail Gateway требуется выполнить первоначальную настройку программы.

kaspersky

В этом разделе

Загрузка ISO-файла

Прежде чем запустить мастер создания виртуальной машины, необходимо загрузить ISO-файл в виртуальное хранилище данных хоста.

► *Чтобы загрузить ISO-файл в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Storage**.
3. Выберите закладку **Datastores**.
4. Нажмите на кнопку **Datastore browser**.

   Откроется окно **Datastore browser**.
5. Выберите хранилище данных и папку, в которую вы хотите загрузить ISO-файл
6. Нажмите на кнопу **Upload**.

   Откроется окно выбора файла.
7. Выберите файл и нажмите **Open**.

Дождитесь загрузки файла. После завершения загрузки имя ISO-файла отобразится в таблице файлов виртуального хранилища данных хоста. Убедитесь, что указанный размер загруженного файла совпадает с размером исходного файла.

Создание виртуальной машины в консоли управления гипервизора VMware ESXi

► *Чтобы создать виртуальную машину в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Virtual Machines**.
3. Нажмите на кнопку **Create/Register VM**.

   Откроется мастер создания виртуальной машины.
4. Следуйте шагам мастера.

   Выберите способ создания виртуальной машины.

1. Выберите вариант **Create a new virtual machine**.

Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Укажите имя виртуальной машины и выберите гостевую операционную систему.

1. В поле **Name** введите имя виртуальной машины.

   Имя должно быть уникальным среди используемых виртуальных машин.

2. В раскрывающемся списке **Compatibility** выберите **ESXi 6.7 U2 virtual machine**.
3. В раскрывающемся списке **Guest OS Family** выберите **Linux**.
4. В раскрывающемся списке **Guest OS Version** выберите **CentOS 7 (64-bit)**.
5. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите виртуальное хранилище данных.

1. Выберите виртуальное хранилище данных из списка доступных хранилищ.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Настройте аппаратную конфигурацию виртуальной машины.

1. На закладке **Virtual Hardware** в блоке параметров **CPU** в раскрывающемся списке выберите количество виртуальных процессоров.

   Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

   Набор доступных значений зависит от возможностей гипервизора.

2. Раскройте блок параметров **Memory** и выполните следующие действия:

   a. В поле **RAM** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

      Минимальное рекомендуемое значение 16 GB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

   b. Установите флажок **Reserve all guest memory (All locked)**.

3. Раскройте блок параметров **Hard Disk 1** и выполните следующие действия:

   a. Укажите объем дискового пространства, которое будет выделено для виртуальной машины.

      Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

   b. В блоке **Disk Provisioning** выберите тип размещения файлов виртуальной машины.

4. В блоке параметров **Network Adapter 1** выберите виртуальную сеть, к которой будет подключена виртуальная машина.

5. В блоке параметров **CD/DVD Drive 1** выполните следующие действия:
   a. Выберите тип привода **Datastore ISO File**.
   b. Нажмите на кнопку **Browse...** справа от поля **CD/DVD Media**.

      Откроется окно выбора файлов.
   c. Выберите ISO-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.
   d. Установите флажок **Connect at power on**.
6. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана.

Изменение параметров виртуальной машины

► *Чтобы изменить параметры виртуальной машины:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** в разделе **Virtual Machines** выберите виртуальную машину, параметры которой вы хотите изменить.
3. В панели управления нажмите на кнопку **Edit**.

   Откроется окно свойств виртуальной машины.
4. На закладке **Virtual Hardware** нажмите на кнопку **Add network adapter**.

   Новый сетевой адаптер отобразится в левой панели.
5. Выберите добавленный сетевой адаптер в левой панели и в раскрывающемся списке справа выберите сегмент сети, к которому он должен быть подключен.
6. Нажмите на кнопку **Save**.

Параметры виртуальной машины будут изменены.

Подключение к виртуальной машине и запуск мастера первоначальной настройки

► *Чтобы подключиться к виртуальной машине и начать настройку Kaspersky Secure Mail Gateway в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** в разделе **Virtual Machines** выберите виртуальную машину, которую вы хотите запустить.
3. Нажмите на кнопку **Power on**.

Виртуальная машина запустится.

4. Нажмите на кнопку **Console** и в раскрывающемся списке выберите требуемый формат запуска консоли:

   - **Open browser console**.
   - **Launch remote console**.

   Откроется консоль управления виртуальной машины. После подключения к виртуальной машине запустится мастер установки и первоначальной настройки программы.

Следуйте указаниям мастера.

Развертывание виртуальной машины в веб-интерфейсе VMware vSphere

Развертывание образа виртуальной машины состоит из следующих этапов:

a. **Загрузка ISO-файла в виртуальное хранилище данных (см. раздел "Загрузка ISO-файла" на стр. 52)**

   ISO-файл Kaspersky Secure Mail Gateway содержит образ операционной системы с предустановленной программой и встроенным почтовым сервером.

b. **Создание виртуальной машины (см. раздел "Создание виртуальной машины в веб-интерфейсе VMware vSphere" на стр. 53)**

   Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Secure Mail Gateway.

c. **Изменение параметров виртуальной машины (на стр. 55)**

   Если вы хотите подключить виртуальную машину к нескольким сегментам сети, вам нужно добавить дополнительный сетевой адаптер для каждого сегмента. Если этого не требуется, вы можете пропустить этот этап.

d. **Подключение к виртуальной машине и запуск мастера первоначальной настройки программы (см. раздел "Подключение к виртуальной машине и начало установки" на стр. 55)**

   Перед началом работы с Kaspersky Secure Mail Gateway требуется выполнить первоначальную настройку программы.

Загрузка ISO-файла

► *Чтобы загрузить ISO-файл в виртуальное хранилище через веб-интерфейс VMware vSphere, выполните следующие действия:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В левой панели нажмите на значок  .

   Откроется страница **Storage**.
3. Выберите хранилище из списка и перейдите на закладку **Files**.
4. Выберите папку, в которую вы хотите загрузить ISO-файл.

5. Нажмите на кнопку **Upload files**.

   Откроется окно выбора файла.

6. Выберите ISO-файл и нажмите на кнопку **Open**.

Дождитесь загрузки файла. После завершения загрузки имя ISO-файла отобразится в таблице файлов виртуального хранилища данных хоста. Убедитесь, что указанный размер загруженного файла совпадает с размером исходного файла.

Создание виртуальной машины в веб-интерфейсе VMware vSphere

► *Чтобы создать виртуальную машину в веб-интерфейсе VMware vSphere, выполните следующие действия:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В левой панели нажмите на значок  .

   Откроется страница **Hosts and clusters**.

3. Выберите центр обработки данных и хранилище, в котором вы хотите создать виртуальную машину.

   В рабочей области отобразится окно свойств выбранного хранилища.

4. В панели управления в раскрывающемся списке **Actions** выберите **New Virtual Machine...**.

   Откроется мастер создания виртуальной машины.

5. Следуйте шагам мастера:

   Выберите способ создания виртуальной машины.

1. Выберите вариант **Create a new virtual machine**.

   Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

   Укажите имя и расположение виртуальной машины.

1. В поле **Virtual machine name** введите имя виртуальной машины.

   > Имя должно быть уникальным среди используемых виртуальных машин.

2. В дереве папок под полем ввода выберите папку в виртуальном хранилище хоста, в которой должна храниться виртуальная машина.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

   Выберите вычислительные ресурсы.

1. В правой части окна мастера выберите кластер и ресурсный пул.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите виртуальное хранилище данных.

1. Выберите виртуальное хранилище данных из списка доступных хранилищ.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Настройте совместимость с виртуальной инфраструктурой.

1. В раскрывающемся списке **Compatible with** выберите **ESXi 6.7 U2 and later**.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите гостевую операционную систему.

1. В раскрывающемся списке **Guest OS Family** выберите **Linux**.
2. В раскрывающемся списке **Guest OS Version** выберите **CentOS 7 (64-bit)**.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Настройте аппаратную конфигурацию виртуальной машины.

1. На закладке **Virtual Hardware** выберите блок параметров **CPU** и в раскрывающемся списке укажите количество виртуальных процессоров.

   Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

   > Набор доступных значений зависит от возможностей гипервизора.

2. Раскройте блок параметров **Memory** и выполните следующие действия:
   a. Укажите объем оперативной памяти, который будет выделен для виртуальной машины.

      Минимальное рекомендуемое значение 16 GB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

   b. Установите флажок **Reserve all guest memory (All locked)**.
3. Раскройте блок параметров **New Hard Disk** и выполните следующие действия:
   a. Укажите объем дискового пространства, которое будет выделено для виртуальной машины.

      Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.

   b. В раскрывающемся списке **Disk Provisioning** выберите тип размещения файлов виртуальной машины.
4. В блоке параметров **New Network** выберите виртуальную сеть, к которой будет подключена виртуальная машина.
5. В блоке параметров **New CD/DVD Drive** выполните следующие действия:
   a. В раскрывающемся списке выберите тип привода **Datastore ISO File**.

      Откроется окно выбора файлов.

b. Выберите ISO-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.

c. В поле **Status** установите флажок **Connect At Power On**.

6. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана и отобразится в списке в левой панели.

Изменение параметров виртуальной машины

► *Чтобы изменить параметры виртуальной машины:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В левой панели нажмите на значок  .

   Откроется страница **Hosts and clusters**.
3. Выберите виртуальную машину, параметры которой вы хотите изменить.
4. В панели управления в раскрывающемся списке **Actions** выберите **Edit Settings...**.

   Откроется окно свойств виртуальной машины.
5. В правом верхнем углу нажмите на кнопку **Add new device** и в раскрывшемся списке выберите **Network adapter**.

   Новый сетевой адаптер отобразится в дереве разделов слева.
6. Выберите добавленный сетевой адаптер в списке разделов и в раскрывающемся списке справа выберите сегмент сети, к которому он должен быть подключен.
7. Нажмите на кнопку **OK**.

Параметры виртуальной машины будут изменены.

Подключение к виртуальной машине и начало установки

► *Чтобы подключиться к виртуальной машине и начать установку Kaspersky Secure Mail Gateway в веб-интерфейсе VMware vSphere, выполните следующие действия:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В левой панели нажмите на значок  .

   Откроется страница **Hosts and clusters**.

3. В контекстном меню виртуальной машины, которую вы хотите запустить, выберите **Power → Power On**.

   Виртуальная машина запустится.

4. В панели управления в раскрывающемся списке **Actions** выберите **Open console**.

   Откроется консоль управления виртуальной машины. После подключения к виртуальной машине запустится мастер установки и первоначальной настройки программы.

Следуйте указаниям мастера.

Развертывание виртуальной машины в консоли управления гипервизора Microsoft Hyper-V Manager

Развертывание образа виртуальной машины состоит из следующих этапов:

a. **Создание виртуальной машины (см. раздел "Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager" на стр. 56)**

b. **Изменение параметров виртуальной машины (на стр. 58)**

   В мастере создания виртуальной машины нет возможности задать некоторые параметры. Поэтому требуется изменить количество виртуальных процессоров, а также параметры безопасной загрузки в уже созданной виртуальной машине.

c. **Подключение к виртуальной машине и запуск мастера первоначальной настройки программы (см. раздел "Подключение к виртуальной машине и запуск мастера первоначальной настройки" на стр. 59)**

   Перед началом работы с Kaspersky Secure Mail Gateway требуется выполнить первоначальную настройку программы.

В этом разделе

Создание виртуальной машины в консоли управления Microsoft Hyper-V Manager

Перед созданием виртуальной машины необходимо разместить ISO-файл в любой сетевой папке, доступной для сервера с гипервизором. Если вы открываете консоль Microsoft Hyper-V Manager на том же сервере, на котором установлен гипервизор, вы можете разместить ISO-файл на локальном жестком диске.

► *Чтобы создать виртуальную машину, выполните следующие действия:*

1. Откройте консоль управления Microsoft Hyper-V Manager.
2. В левой части окна выберите для подключения гипервизор, на котором вы хотите развернуть образ виртуальной машины.
3. В контекстном меню выберите пункт **New** → **Virtual Machine**.

   Откроется мастер создания виртуальной машины.
4. Следуйте шагам мастера:

   Выберите имя и расположение виртуальной машины.

1. Введите имя новой виртуальной машины в поле **Name**.

   Имя должно быть уникальным среди используемых виртуальных машин.

2. Если вы хотите изменить папку для сохранения виртуальной машины, выполните следующие действия:

   a. Установите флажок **Store the virtual machine in a different location**.

   b. В поле **Location** укажите путь к папке, в которой вы хотите сохранить виртуальную машину.

   По умолчанию выбрана папка <диск>:\Virtual Machines.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите поколение виртуальной машины.

1. Выберите один из следующих вариантов:
   - **Generation 1**, если вы используете гипервизор Microsoft Hyper-V Server 2016.
   - **Generation 2**, если вы используете гипервизор Microsoft Hyper-V Server 2019 или 2022.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выделите память для виртуальной машины.

1. В поле **Startup memory** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

   Минимальное рекомендуемое значение 16384 MB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.
2. Снимите флажок **Use Dynamic Memory for this virtual machine**.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Настройте сетевое подключение.

1. В раскрывающемся списке **Connection** выберите виртуальную сеть, к которой будет подключена виртуальная машина.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Подключите виртуальный жесткий диск.

1. Выберите пункт **Create a virtual hard disk**.
2. В поле **Name** укажите имя создаваемого виртуального диска.
3. В поле **Location** выберите место хранения данных создаваемого виртуального диска на физическом сервере.
4. В поле **Size** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

   Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.
5. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите способ установки операционной системы.

1. В списке действий выберите **Install an operating system from a bootable image file**.
2. В блоке параметров **Media** в поле **Image file (.iso)** укажите путь к установочному ISO-образу виртуальной машины.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Finish**.

Виртуальная машина с заданными параметрами будет создана. Убедитесь, что она отображается в списке **Virtual Machines** на выбранном гипервизоре.

Виртуальная машина создается с количеством процессоров, установленным по умолчанию. Вам требуется изменить этот параметр в свойствах виртуальной машины после ее создания.

Изменение параметров виртуальной машины

Перед выполнением этой инструкции убедитесь, что виртуальная машина выключена.

Для корректной работы программы требуется изменить количество процессоров виртуальной машины, а также настроить параметры безопасной загрузки.

► *Чтобы изменить параметры виртуальной машины, выполните следующие действия:*

1. Запустите программу Hyper-V Manager.
2. В главном окне программы в таблице **Virtual Machines** выберите виртуальную машину, развернутую из ISO-файла.

3. По правой кнопке мыши откройте контекстное меню и выберите пункт **Settings**.

   Откроется окно свойств виртуальной машины.

4. В блоке параметров **Security** в раскрывающемся списке **Template** выберите **Microsoft UEFI Certificate Authority**.

   Применимо только для виртуальных машин второго поколения.

5. В блоке параметров **Hardware** выберите раздел **Processor**.
6. В поле **Number of virtual processors** укажите количество виртуальных процессоров.

   Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.

7. Если требуется подключить виртуальную машину к нескольким сегментам сети, добавьте дополнительные сетевые адаптеры. Для этого выполните следующие действия:

   a. В блоке параметров **Hardware** выберите раздел **Add Hardware**.

   b. В рабочей области выберите **Network Adapter** и нажмите на кнопку **Add**.

      Новый сетевой адаптер отобразится в конце списка в блоке **Hardware**.

   c. Выберите новый сетевой адаптер в блоке **Hardware** и в раскрывающемся списке **Virtual switch** выберите сегмент сети, к которому вы хотите его подключить.

8. Нажмите на кнопку **OK**.

Количество процессоров виртуальной машины будет изменено.

Подключение к виртуальной машине и запуск мастера первоначальной настройки

► *Чтобы подключиться к виртуальной машине и начать настройку Kaspersky Secure Mail Gateway в консоли управления Microsoft Hyper-V Manager, выполните следующие действия:*

1. Откройте консоль управления Microsoft Hyper-V Manager
2. В левой части окна выберите гипервизор, на котором развернута виртуальная машина.
3. В рабочей области щелкните правой клавишей мыши по виртуальной машине, которую вы хотите запустить.
4. В контекстном меню выберите команду **Start**.

   Виртуальная машина запустится.

5. В контекстном меню виртуальной машины выберите команду **Connect**.

Откроется консоль управления виртуальной машины и запустится мастер установки и первоначальной настройки. Следуйте указаниям мастера.

kaspersky

Развертывание виртуальной машины с помощью программы Microsoft SCVMM

Развертывание образа виртуальной машины состоит из следующих этапов:

a. **Загрузка ISO-файла в библиотеку сервера Microsoft SCVMM (см. раздел "Загрузка ISO-файла" на стр. 60)**

   ISO-файл Kaspersky Secure Mail Gateway содержит образ операционной системы с предустановленной программой и встроенным почтовым сервером.

b. **Создание виртуальной машины (см. раздел "Создание виртуальной машины с помощью программы Microsoft SCVMM" на стр. 61)**

   Во время создания виртуальной машины требуется установить значения параметров, рекомендуемые для работы Kaspersky Secure Mail Gateway.

c. **Изменение параметров виртуальной машины (на стр. 63)**

   Если вы хотите подключить виртуальную машину к нескольким сегментам сети, вам нужно добавить дополнительный сетевой адаптер для каждого сегмента. Если этого не требуется, вы можете пропустить этот этап.

d. **Подключение к виртуальной машине и запуск мастера первоначальной настройки программы (см. раздел "Подключение к виртуальной машине и запуск мастера первоначальной настройки" на стр. 64)**

   Перед началом работы с Kaspersky Secure Mail Gateway требуется выполнить первоначальную настройку программы.

В этом разделе

Загрузка ISO-файла

Для загрузки ISO-файла в библиотеку сервера Microsoft SCVMM необходимо разместить его на локальном жестком диске того компьютера, на котором запускается программа Microsoft SCVMM.

► *Чтобы загрузить ISO-файл в библиотеку сервера Microsoft SCVMM, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левой нижней части окна выберите раздел **Library**.
3. В панели управления нажмите на кнопку **Import Physical Resource**.

Откроется окно **Import Library Resources**.

4. Нажмите на кнопку **Browse...**.

   Откроется окно **Select Destination Folder**.

5. Выберите библиотеку ресурсов и папку, в которую будет загружен ISO-файл, и нажмите на кнопку **OK**.
6. В окне **Import Library Resources** нажмите на кнопку **Add resource...**.

   Откроется окно **Select resource items**.

7. Выберите ISO-файл и нажмите на кнопку **Open**.
8. Нажмите на кнопку **Import**.

ISO-файл будет загружен в библиотеку сервера Microsoft SCVMM и отобразится в таблице **Physical Library Objects**.

Создание виртуальной машины с помощью программы Microsoft SCVMM

Если гипервизор Microsoft Hyper-V подключен к инфраструктуре Microsoft System Center, то вы можете создать виртуальную машину с помощью программы Microsoft SCVMM.

► *Чтобы создать виртуальную машину, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левом нижнем углу окна выберите раздел **VMs and Services**.
3. В панели инструментов нажмите на кнопку **Create Virtual Machine** и в раскрывающемся списке выберите пункт **Create Virtual Machine**.

   Откроется мастер создания виртуальной машины.

4. Следуйте шагам мастера:

   Выберите способ создания виртуальной машины.

1. Выберите вариант **Create the new virtual machine with a blank virtual hard disk**.

   Этот способ позволяет вручную настроить параметры и аппаратную конфигурацию виртуальной машины.

2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Укажите имя и поколение виртуальной машины.

1. В поле **Virtual machine name** введите имя виртуальной машины.

   Имя должно быть уникальным среди используемых виртуальных машин.

2. В раскрывающемся списке **Generation** выберите один из следующих вариантов:
   - **Generation 1**, если вы используете гипервизор Microsoft Hyper-V Server 2016.
   - **Generation 2**, если вы используете гипервизор Microsoft Hyper-V Server 2019 или 2022.

3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Настройте аппаратную конфигурацию виртуальной машины.

1. В разделе **Compatibility** установите флажок **Hyper-V**.
2. В блоке параметров **General** в разделе **Processor** укажите количество виртуальных процессоров в поле **Number of processors**.

   Минимальное рекомендуемое значение 8. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.
3. В блоке параметров **General** в разделе **Memory** выполните следующие действия:
   a. Выберите вариант **Static**.
   b. В поле **Virtual machine memory** укажите объем оперативной памяти, который будет выделен для виртуальной машины.

      Минимальное рекомендуемое значение 16384 MB. Вы можете указать большее значение, если вам требуется более высокая производительность виртуальной машины.
4. В блоке параметров **Bus configuration** в разделе **SCSI Adapter** → **<название диска>** выполните следующие действия:
   a. Выберите вариант **Create a new virtual hard disk**.
   b. В раскрывающемся списке **Type** выберите тип виртуального диска **Fixed**.
   c. В поле **Size** укажите объем дискового пространства, которое будет выделено для виртуальной машины.

      Минимальное рекомендуемое значение 200 GB. Вы можете указать большее значение, если вам требуется хранить большую базу данных для журнала событий.
5. В блоке параметров **Bus configuration** в разделе **SCSI Adapter** → **Virtual DVD Drive** выберите тип носителя виртуального диска. Для этого выполните следующие действия:
   a. Выберите вариант **Existing ISO image**.
   b. Нажмите на кнопку **Browse...**.

      Откроется окно **Select ISO**.
   c. Выберите ISO-файл, загруженный перед началом установки программы, и нажмите на кнопку **OK**.
6. В блоке параметров **Network Adapters** в разделе **Network Adapter 1** выполните следующие действия:
   a. Выберите режим подключения сетевого адаптера **Connected to a VM network**.
   b. Справа от поля **VM network** нажмите на кнопку **Browse...**.

      Откроется окно **Select a VM Network**.
   c. Выберите виртуальную сеть, к которой будет подключена виртуальная машина, и нажмите на кнопку **OK**.
7. В блоке параметров **Advanced** выберите раздел **Firmware** и снимите флажок **Enable secure boot**.

   Применимо только для виртуальных машин второго поколения.
8. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите тип размещения виртуальной машины.

1. Выберите вариант **Place the virtual machine on a host**.
2. В раскрывающемся списке **Destination** выберите группу хостов для создания виртуальной машины.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера

Выберите гипервизор, на котором будет создана виртуальная машина.

1. В таблице гипервизоров группы, выбранной на предыдущем шаге, выберите гипервизор, на котором будет размещена виртуальная машина.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Проверьте правильность заданных значений параметров.

1. Проверьте параметры виртуальной машины, заданные на предыдущих шагах мастера.
2. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Выберите операционную систему и настройте дополнительные параметры.

1. В раскрывающемся списке **Action to take when the virtualization server stops** выберите **Shut down guest OS**.
2. В блоке параметров **Operating system** в раскрывающемся списке выберите **CentOS Linux 7 (64 bit)**.
3. Нажмите на кнопку **Next**.

Вы перейдете к следующему шагу мастера.

Подтвердите создание виртуальной машины.

1. Проверьте правильность параметров виртуальной машины, настроенных на предыдущих шагах.
2. Если все параметры установлены правильно, нажмите на кнопку **Create**.

Запустится процесс создания виртуальной машины с заданными параметрами. Убедитесь, что процесс завершен корректно и виртуальная машина отображается в списке виртуальных машин выбранного гипервизора.

Изменение параметров виртуальной машины

► *Чтобы изменить параметры виртуальной машины:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левой нижней части окна выберите раздел **VMs and Services**.
3. В левой верхней части окна в дереве выберите гипервизор, на котором была создана виртуальная машина.
4. В рабочей области окна выберите виртуальную машину, параметры которой вы хотите изменить.
5. В контекстном меню выберите пункт **Properties**.

   Откроется окно свойств виртуальной машины.
6. В левой панели выберите раздел **Hardware Configuration**.

7. В верхней панели управления нажмите на кнопку **New** и в раскрывшемся списке выберите **Network adapter**.

   Новый сетевой адаптер отобразится в блоке параметров **Network Adapters**.

8. В рабочей области выполните следующие действия:

   a. Выберите режим подключения сетевого адаптера **Connected to a VM network**.

   b. Справа от поля **VM network** нажмите на кнопку **Browse...**.

      Откроется окно **Select a VM Network**.

   c. Выберите сегмент сети, к которому должен быть подключен добавленный сетевой адаптер, и нажмите на кнопку **OK**.

9. Нажмите на кнопку **OK**.

Параметры виртуальной машины будут изменены.

Подключение к виртуальной машине и запуск мастера первоначальной настройки

► *Чтобы подключиться к виртуальной машине и начать настройку Kaspersky Secure Mail Gateway с помощью программы Microsoft SCVMM, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левой нижней части окна выберите раздел **VMs and Services**.
3. В левой верхней части окна в дереве выберите гипервизор, на котором была создана виртуальная машина.
4. В рабочей области окна выберите виртуальную машину, которую вы хотите запустить.
5. В панели инструментов нажмите на кнопку **Power On**.

   Виртуальная машина запустится.

6. В панели инструментов нажмите на кнопку **Connect or View** и в раскрывающемся списке выберите пункт **Connect via Console**.

Откроется консоль управления виртуальной машины и запустится мастер установки и первоначальной настройки. Следуйте указаниям мастера.

kaspersky

Развертывание образа виртуальной машины в гипервизоре KVM

Этот раздел содержит пошаговые инструкции по развертыванию образа виртуальной машины Kaspersky Secure Mail Gateway в гипервизоре KVM.

В этом разделе

Шаг 1. Выбор метода установки операционной системы

► *Чтобы выбрать метод установки операционной системы, выполните следующие действия:*

1. На сервере с гипервизором KVM запустите программу Менеджер виртуальных машин (Virtual Machine Manager).

   В главном окне программы отобразится список доступных гипервизоров.

2. В контекстном меню нужного гипервизора выберите пункт **Создать**.

   Запустится мастер создания виртуальной машины.

3. Выберите вариант **Локальный ISO или CDROM** и нажмите на кнопку **Вперед**.

Вы перейдете к следующему шагу мастера.

Шаг 2. Выбор расположения установочного носителя

Требуется предварительно загрузить ISO-файл, содержащий образ виртуальной машины, в локальную папку сервера с гипервизором KVM.

► *Чтобы выбрать расположение установочного носителя, выполните следующие действия:*

1. Выберите вариант **Образ ISO**.
2. С помощью кнопки **Обзор** укажите путь к ISO-файлу, содержащему образ виртуальной машины.
3. Снимите флажок **Автоматически определить операционную систему носителя**.
4. В раскрывающемся списке **Тип** выберите **Linux**.

5. В раскрывающемся списке **Версия** выберите **CentOS 7.0**.
6. Нажмите на кнопку **Вперед**.

Вы перейдете к следующему шагу мастера.

Шаг 3. Настройка памяти и процессоров

► *Чтобы настроить параметры памяти и процессоров виртуальной машины, выполните следующие действия:*

1. В поле **Память (ОЗУ)** укажите 16384 (МБ).
2. В поле **Процессоры** укажите 8.
3. Нажмите на кнопку **Вперед**.

Вы перейдете к следующему шагу мастера.

Шаг 4. Настройка параметров жесткого диска

► *Чтобы настроить параметры жесткого диска, выполните следующие действия:*

1. Установите флажок **Настроить пространство хранения данных**.
2. Выберите пункт **Создать образ диска для виртуальной машины**.
3. В поле ниже укажите 200 (ГБ), чтобы задать размер виртуального жесткого диска.
4. Нажмите на кнопку **Вперед**.

Вы перейдете к следующему шагу мастера.

Шаг 5. Назначение имени виртуальной машины и настройка сетевых параметров

► *Чтобы назначить имя виртуальной машины и настроить сетевые параметры, выполните следующие действия:*

1. В поле **Название** введите любое имя, под которым виртуальная машина будет отображаться в консоли управления гипервизором.
2. Установите флажок **Проверить конфигурацию перед установкой**.
3. В раскрывающемся списке **Выбор сети** выберите предварительно настроенную виртуальную сеть или сетевой адаптер хоста.
4. В раскрывающемся списке **Режим** выберите **Мост**.
5. Нажмите на кнопку **Готово**.

Откроется окно с заданными параметрами виртуальной машины.

Шаг 6. Настройка дополнительных параметров виртуальной машины

► *Чтобы настроить дополнительные параметры виртуальной машины и запустить установку, выполните следующие действия:*

1. В левой панели выберите раздел **Диск 1**.
2. Раскройте блок **Дополнительные параметры**.
3. В раскрывающемся списке **Шина диска** выберите **SCSI**.
4. Нажмите на кнопку **Применить**.
5. В левой панели выберите раздел **Дисплей**.
6. В раскрывающемся списке **Тип** выберите один из следующих вариантов:
   - **VNC-сервер**;
   - **Сервер SPICE**.
7. Нажмите на кнопку **Применить**.
8. В верхней панели нажмите на кнопку **Начать установку**.

Виртуальная машина будет создана.

Установка и первоначальная настройка программы

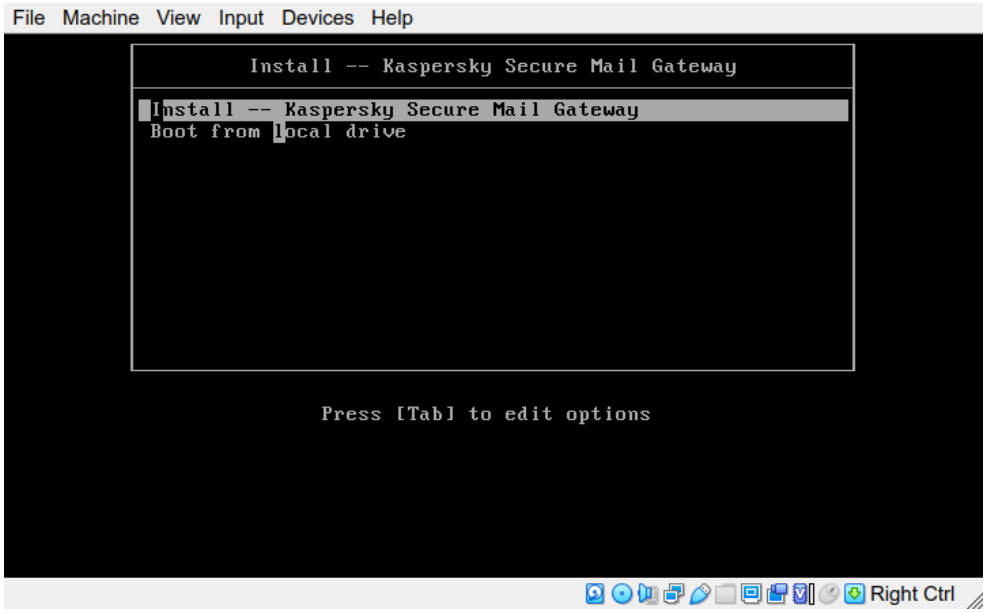
Данная инструкция описывает процесс установки и первоначальной настройки программы на виртуальной машине, использующей загрузчик BIOS. На виртуальных машинах с UEFI псевдографический интерфейс может отличаться.

► *Чтобы установить и настроить программу, выполните следующие действия:*

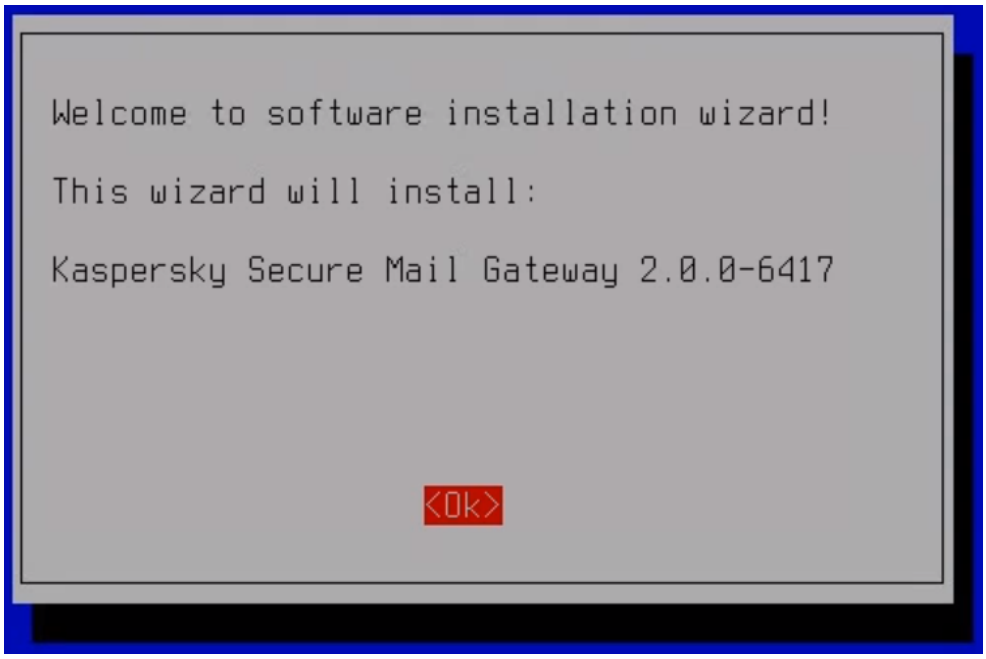
1. Запустите подготовленную виртуальную машину или физический сервер и выберите загрузку с CD-диска.

   Начнется загрузка с ISO-образа диска.

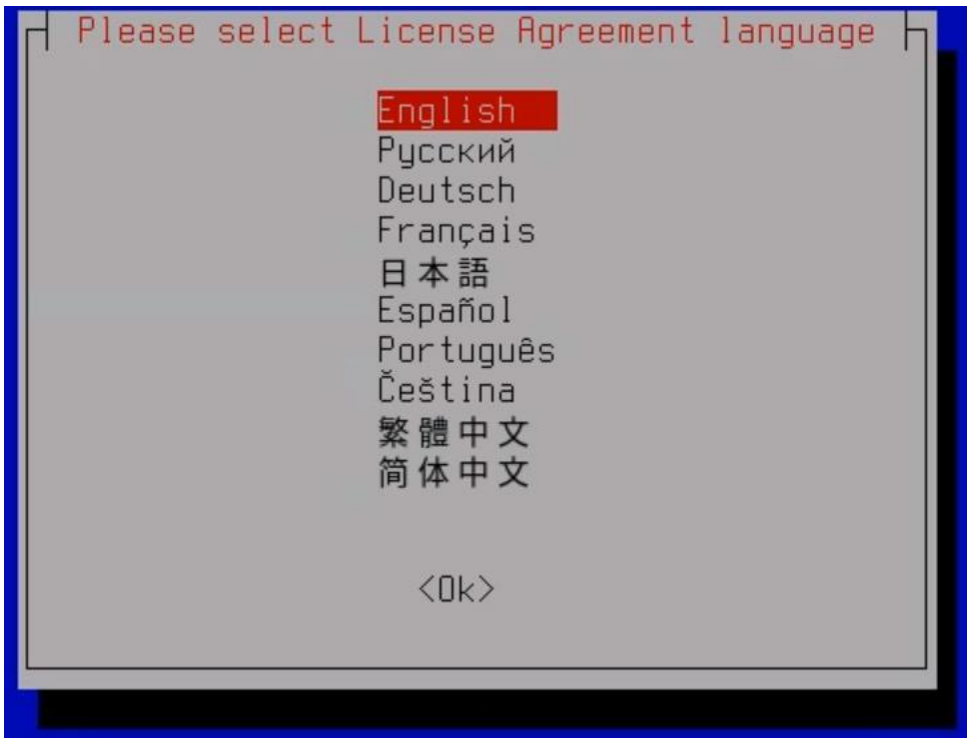
2. В следующем окне выберите **Install -- Kaspersky Secure Mail Gateway** или дождитесь, пока загрузка операционной системы и мастера установки начнется автоматически.



3. В приветственном окне мастера установки нажмите на кнопку **Ok**.



4. Выберите язык просмотра Лицензионного соглашения и Политики конфиденциальности.



5. Выразите свое согласие или несогласие с Лицензионным соглашением. Для этого выполните следующие действия:

   - Если вы хотите принять условия Лицензионного соглашения, нажмите на кнопку **I accept** (Я принимаю).
   - Если вы хотите отклонить условия Лицензионного соглашения, нажмите на кнопку **I decline** (Я отклоняю).

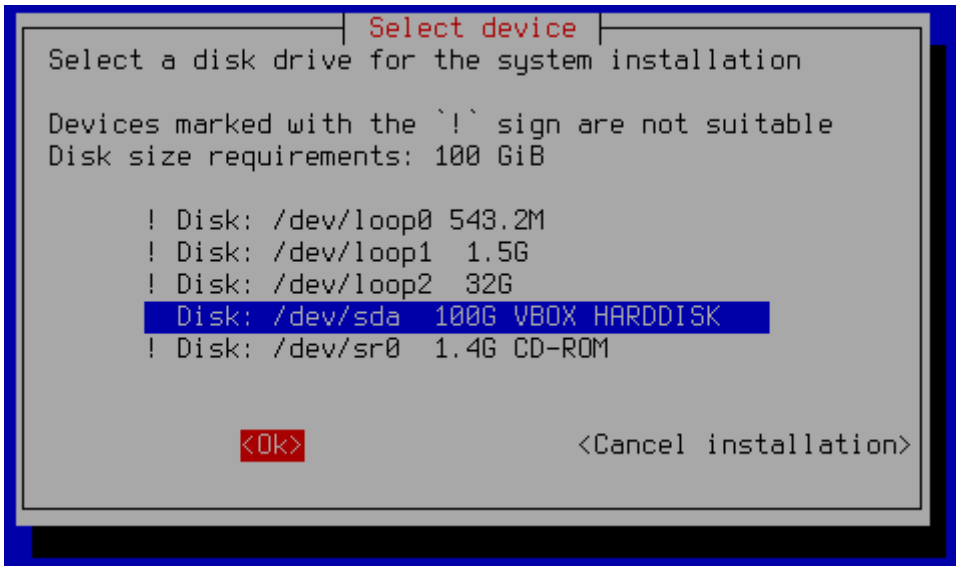
   Если вы отклонили условия Лицензионного соглашения, установка программы не выполняется.

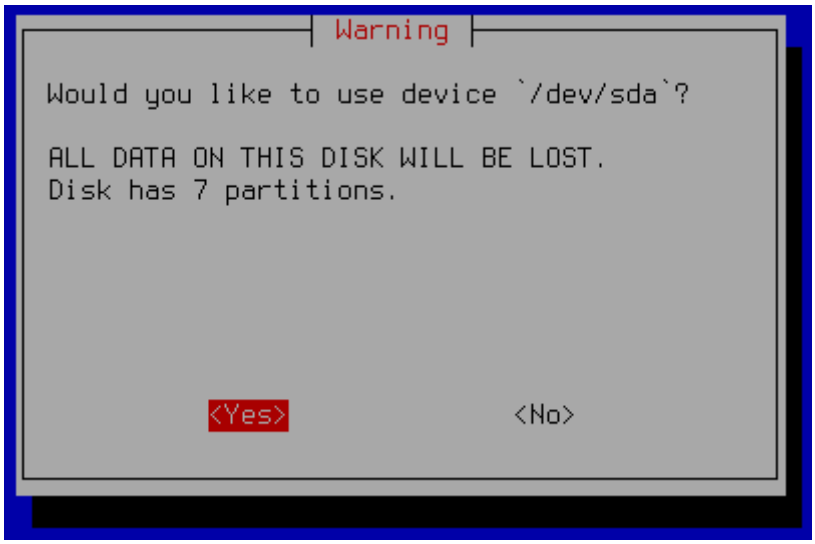
6. Выразите свое согласие или несогласие с Политикой конфиденциальности. Для этого выполните следующие действия:

   - Если вы хотите принять условия Политики конфиденциальности, нажмите на кнопку **I accept** (Я принимаю).
   - Если вы хотите отклонить условия Политики конфиденциальности, нажмите на кнопку **I decline** (Я отклоняю).

   Если вы отклонили условия Политики конфиденциальности, установка программы не выполняется.

7. Выберите диск, на котором будет установлена программа и в окне подтверждения нажмите на кнопку **Yes**.



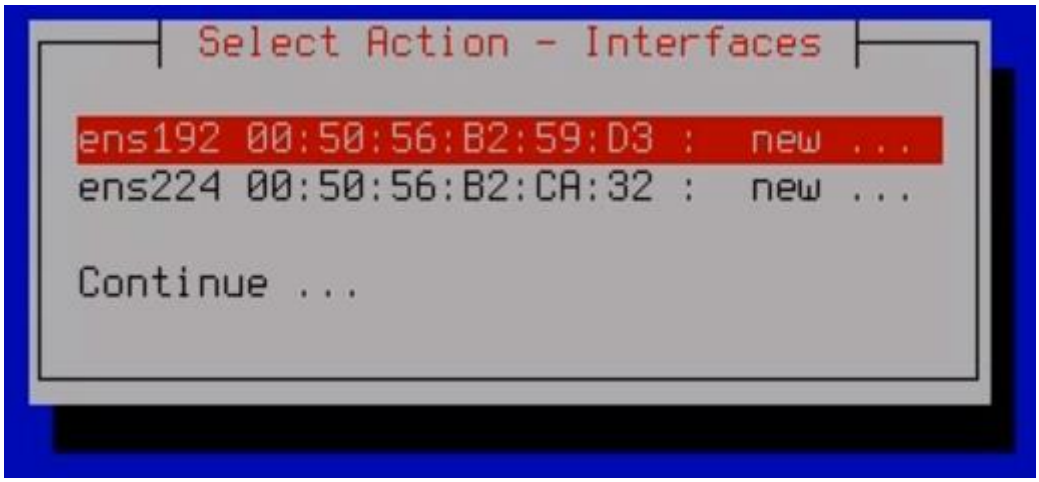


Дождитесь, пока данные ISO-образа скопируются на виртуальный диск. После завершения копирования виртуальная машина будет перезагружена и запустится мастер первоначальной настройки программы.

8. В открывшемся окне **Hostname** в поле **Hostname** укажите полное доменное имя сервера с установленной программой Kaspersky Secure Mail Gateway, указанное на DNS-сервере, и нажмите на кнопку **OK**.

Откроется окно со списком доступных сетевых адаптеров.

9. Выберите сетевой адаптер, параметры которого вы хотите настроить, и нажмите клавишу **ENTER**.

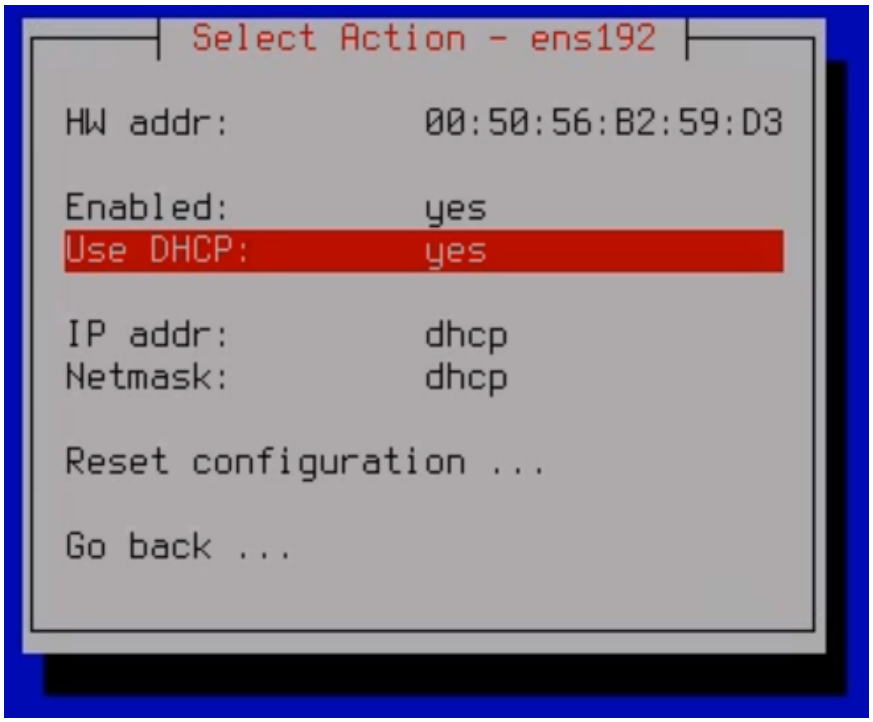


Если вы выполняете первоначальную настройку впервые и адаптер не был инициализирован ранее, то откроется окно подтверждения инициализации.

10. В окне подтверждения нажмите на кнопку **Yes**. Статус адаптера сменится с *new* на *on*. Выберите адаптер в списке и нажмите клавишу **ENTER**.

Откроется окно со свойствами адаптера.

11. Настройте режим работы протоколов IPv4 и IPv6. Для этого переведите курсор в строку Use DHCP и нажмите клавишу **ENTER**.

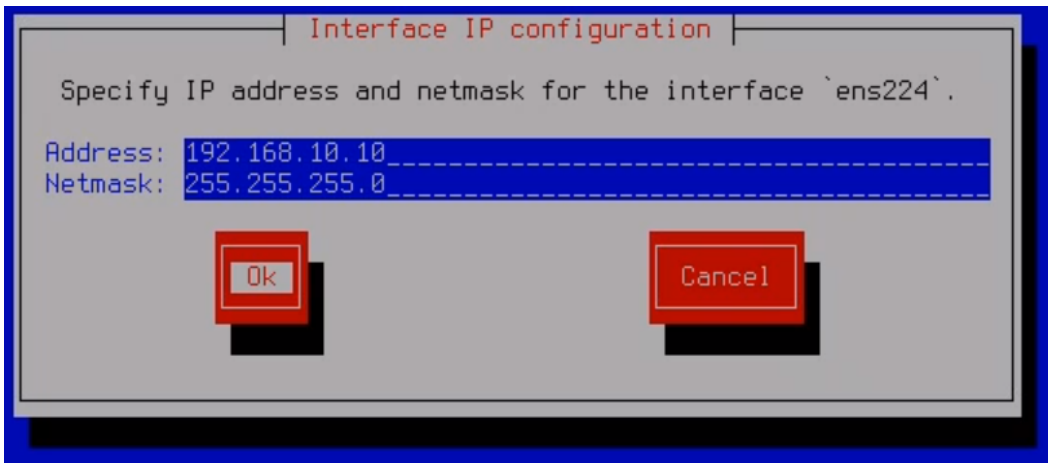


12. В открывшемся окне выберите режим:
    - Если вы хотите использовать статический IP-адрес для сервера с установленной программой, нажмите на кнопку **Yes**.
    - Если вы хотите, чтобы параметры сетевого адаптера были получены по протоколу DHCP, нажмите на кнопку **No**.

    По умолчанию используется протокол DHCP. Этот режим подойдет для установки программы в тестовых целях или для демонстрации. Для корректной работы кластера в реальной инфраструктуре рекомендуется использовать статическую конфигурацию.

13. Если на предыдущем шаге вы выбрали статическую конфигурацию, в открывшемся окне **Interface IP configuration** выполните следующие действия:
    a. В поле **Addresses** укажите IP-адрес сетевого адаптера.
    b. В поле **Netmask** укажите маску сети.

c. Нажмите **OK**, чтобы сохранить внесенные изменения.

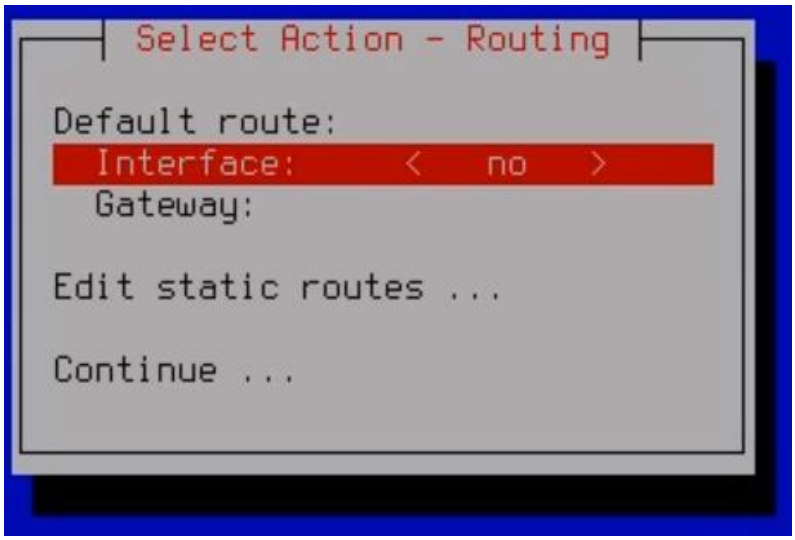


d. Нажмите на кнопку **Go back** внизу окна после завершения настройки сетевого адаптера.

Откроется окно со списком всех доступных сетевых адаптеров. При необходимости вы можете повторить настройку для другого адаптера.

14. После завершения настройки всех сетевых адаптеров выберите **Continue** внизу списка.

Откроется окно **Select Action – Routing**.



15. Чтобы настроить маршрут по умолчанию, выполните следующие действия:

a. Выберите пункт **Interface** и нажмите клавишу **ENTER**.

b. В открывшемся окне **Select gateway device** выберите сетевой адаптер, который должен использоваться для маршрута по умолчанию, и нажмите на клавишу **ENTER**.

c. Если на предыдущем шаге вы выбрали сетевой адаптер, использующий протокол DHCP, в поле **Gateway** автоматически будет установлено значение **dhcp**. Если вы выбрали сетевой адаптер со статической конфигурацией, опция **dhcp** для шлюза по умолчанию будет недоступна.

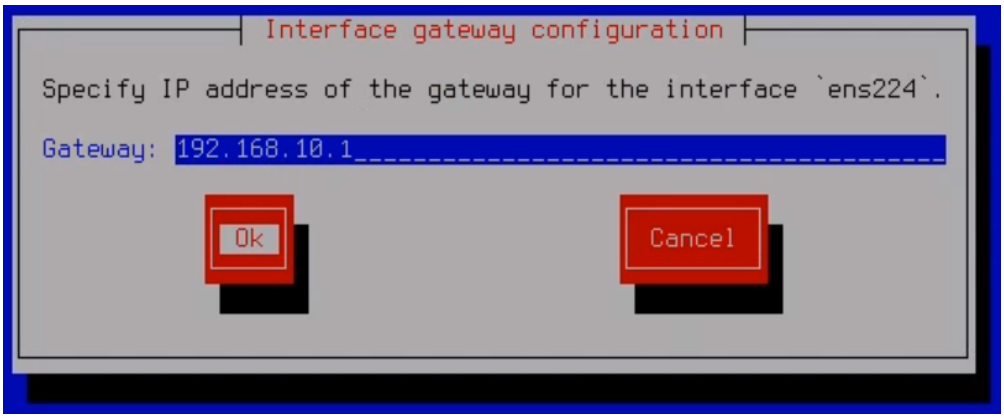
d. Чтобы задать статический IP-адрес шлюза по умолчанию, выполните следующие действия:

1. Выберите пункт **Gateway** и нажмите на клавишу **ENTER**.

2. Для адаптеров, использующих протокол DHCP, в открывшемся окне **Use static configuration** нажмите на кнопку **Yes**.

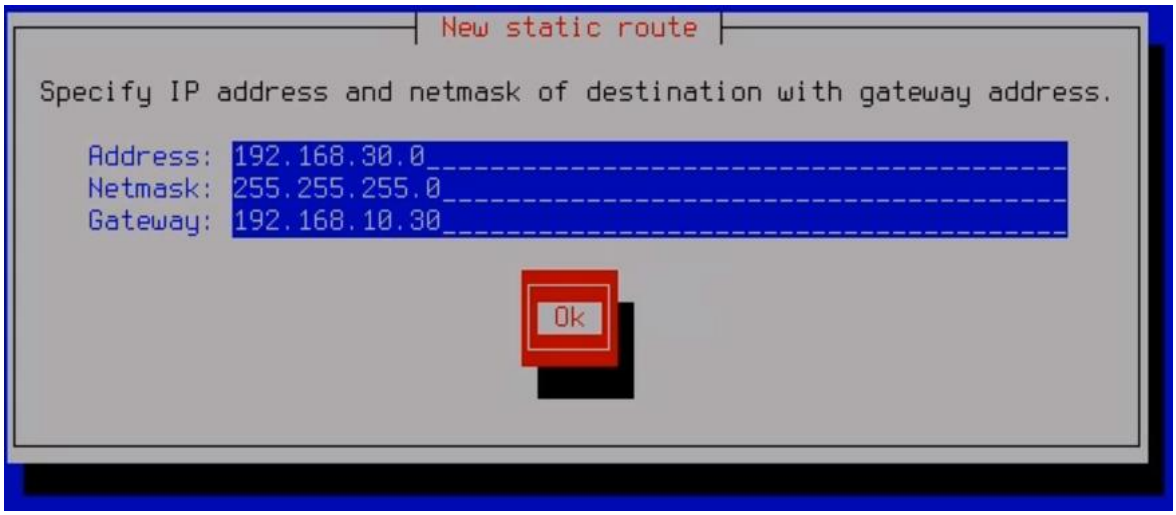
Откроется окно **Interface gateway configuration**.

3. В поле **Gateway** введите статический адрес шлюза по умолчанию и нажмите на кнопку **Ok**.



16. Если требуется, вы можете настроить статический маршрут. Для этого выполните следующие действия:
    a. В окне **Select Action – Routing** выберите пункт **Edit static routes** и нажмите клавишу **ENTER**.
    b. В открывшемся окне **Select Action – Routes** нажмите **New route**.

       Откроется окно **New static route**.
    c. В поле **Address** укажите IP-адрес сетевого адаптера.
    d. В поле **Netmask** укажите маску сети.
    e. В поле **Gateway** укажите IP-адрес шлюза.
    f. Нажмите на кнопку **Ok**.



g. В открывшемся окне выберите сетевой адаптер, через который будет проходить статический маршрут, и нажмите клавишу **ENTER**.

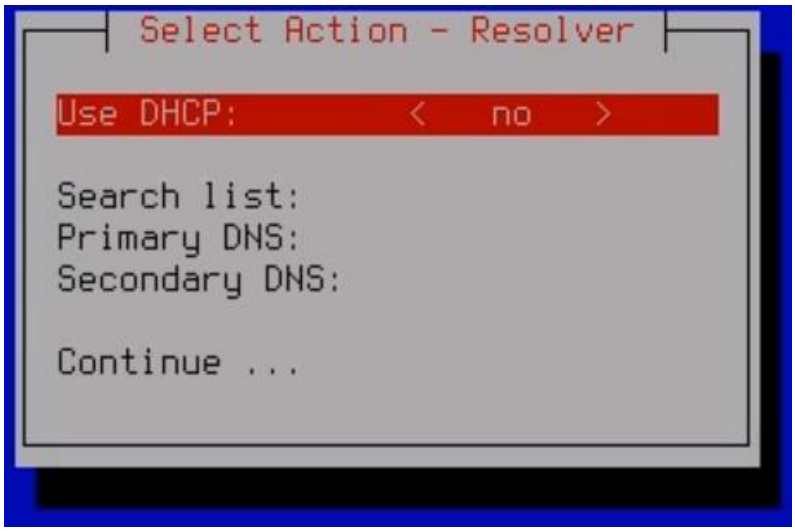
Добавленный статический маршрут отобразится в окне **Select Action – Routes**.

При необходимости вы можете повторить шаги b – g для добавления еще одного статического маршрута.

h. После завершения настройки нажмите **Go back** в нижней части окна **Select Action – Routes**.

i. Нажмите **Continue** в нижней части окна **Select Action – Routing**.

Откроется окно **Select Action – Resolver**.



17. Если вы хотите получать адреса серверов DNS, а также список поиска DNS-суффиксов по протоколу DHCP, выполните следующие действия:

a. В поле **Use DHCP** нажмите на клавишу **ENTER**.

Откроется окно **Obtain DNS addresses over DHCP**.

b. Выберите сетевой интерфейс службы DHCP.

Значения полей **Search list**, **Primary DNS** и **Secondary DNS** будут заполнены автоматически.

c. В окне **Select Action – Resolver** нажмите на кнопку **Continue**.

18. Если вы хотите настроить параметры службы DNS вручную, выполните следующие действия:

a. Убедитесь, что в поле **Use DHCP** установлен вариант **no**.

b. В поле **Search list** нажмите на клавишу **ENTER**.

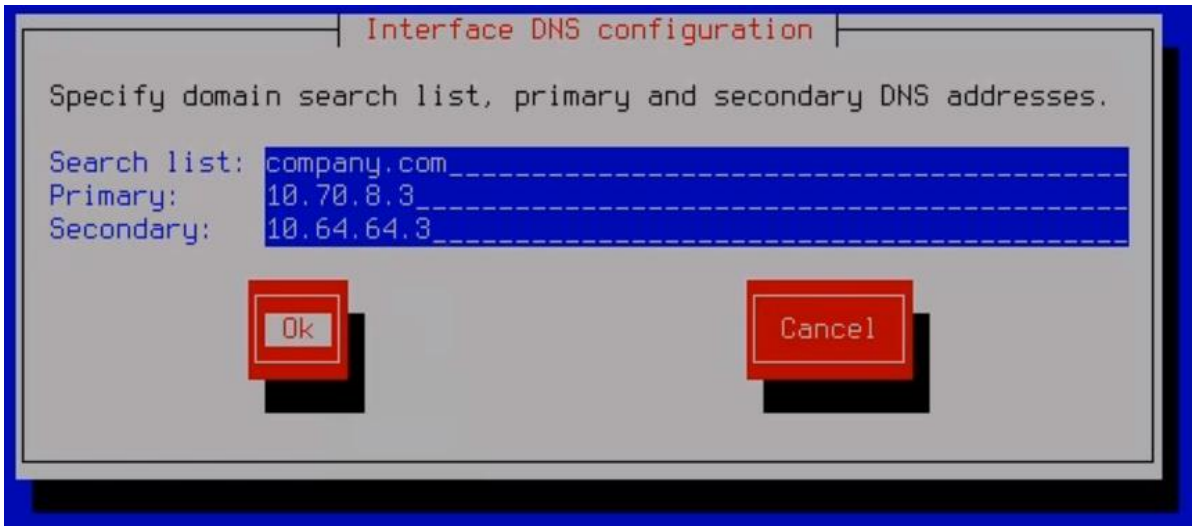
Откроется окно **Interface DNS configuration**.

c. В поле **Search list** введите DNS-суффикс поиска доменов.

d. В поле **Primary** введите адрес первичного DNS-сервера.

e. В поле **Secondary** введите адрес вторичного DNS-сервера.

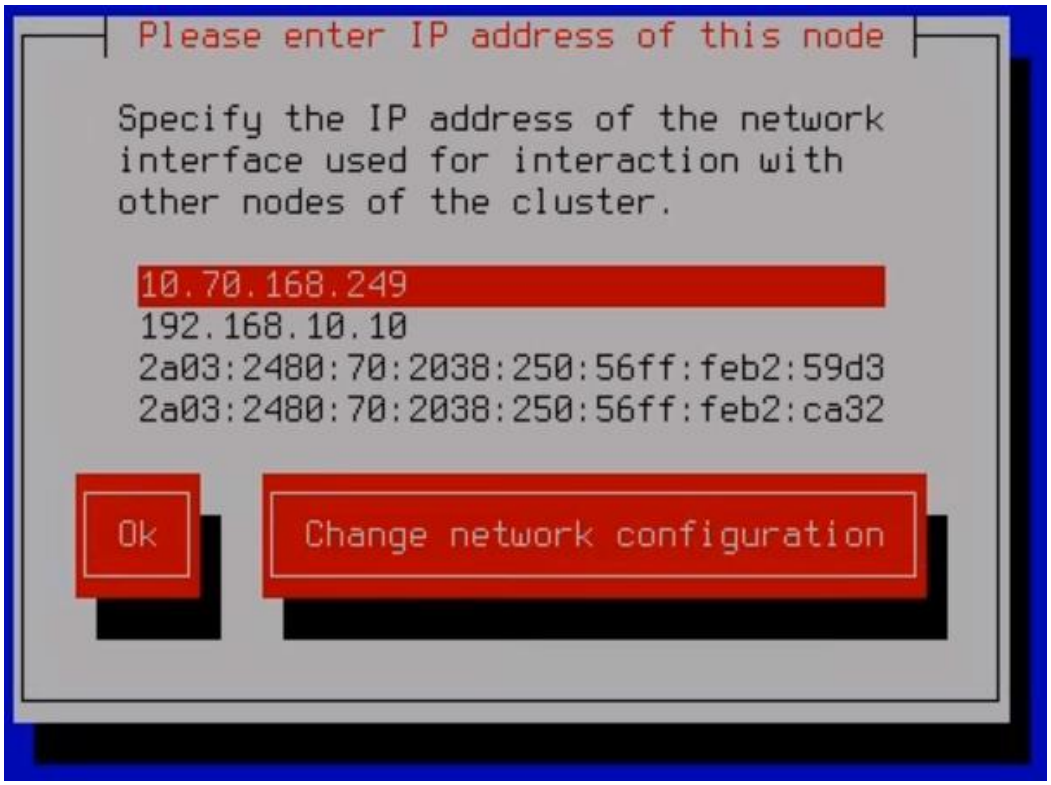
f. Нажмите на кнопку **OK**.



g. В окне **Select Action – Resolver** нажмите на кнопку **Continue**.

Откроется следующее окно мастера первоначальной настройки.

19. Выберите IP-адрес сетевого интерфейса для приема входящего соединения для взаимодействия с другими узлами кластера. Нажмите на кнопку **OK**.



20. Укажите порт для взаимодействия с другими узлами кластера и нажмите на кнопку **OK**.

Рекомендуется использовать значение по умолчанию: 9045.

21. Задайте пароль Локального администратора.

Пароль должен содержать:

- минимум 15 символов;
- только символы ASCII (A-Z, a-z), цифры и специальные символы;

- символы следующих типов:
  - символ верхнего регистра (A-Z);
  - символ нижнего регистра (a-z);
  - цифру;
  - специальный символ.

22. Сохраните любым удобным для вас способом отпечаток сертификата сервера, который отобразится в завершающем окне мастера настройки.

При добавлении сервера в кластер (см. раздел "Добавление узла в кластер" на стр. 132) через веб-интерфейс программы вам потребуется сверить этот отпечаток с отпечатком, отображаемым в веб-интерфейсе.

Установка и первоначальная настройка программы будут завершены. После этого вы сможете подключиться к веб-интерфейсу программы через браузер для настройки ее параметров.

После завершения первоначальной настройки рекомендуется отключить загрузку с диска, содержащего ISO-образ, в свойствах виртуальной машины.

Удаление программы

После удаления программы вся информация, связанная с ней, будет потеряна.

Для программы не предусмотрено стандартной процедуры удаления.

Вы можете удалить всю виртуальную машину, в том числе файлы виртуальных дисков и файлы снимков состояния системы. Для этого следуйте указаниям одной из инструкций этого раздела в зависимости от используемого гипервизора.

Если вы развернули программу на физическом сервере, для удаления программы вам потребуется отформатировать жесткий диск сервера с помощью специализированной утилиты для удаления данных и убедиться, что загрузка программы стала невозможна.

В этом разделе

Подготовка к удалению программы

Перед удалением программы с физического сервера или виртуальной машины требуется выполнить следующие действия:

a. **Отключить балансировку нагрузки для удаляемого узла кластера**

b. **Остановить поступление запросов на обработку трафика**

   Для этого убедитесь, что обработка трафика перенаправлена в обход удаляемого узла кластера.

c. **Удалить узел из кластера (см. раздел "Удаление узла из кластера" на стр. 133)**

kaspersky

Удаление виртуальной машины в консоли управления гипервизора VMware ESXi

Перед удалением программы требуется выполнить подготовительные действия.

► *Чтобы удалить виртуальную машину в консоли управления гипервизора VMware ESXi, выполните следующие действия:*

1. Откройте консоль управления гипервизора VMware ESXi.
2. В панели **Navigator** выберите раздел **Virtual Machines**.
3. В рабочей области выберите виртуальную машину, которую вы хотите удалить.
4. Если виртуальная машина включена, отключите ее. Для этого нажмите на кнопку **Power off**. Дождитесь отключения машины.
5. В панели управления в раскрывающемся списке **Actions** выберите **Delete**.
6. В окне подтверждения нажмите на кнопку **Delete**.

Виртуальная машина с установленной программой Kaspersky Secure Mail Gateway будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины в веб-интерфейсе VMware vSphere

Перед удалением программы требуется выполнить подготовительные действия.

► *Чтобы удалить виртуальную машину в веб-интерфейсе VMware vSphere, выполните следующие действия:*

1. В веб-интерфейсе программы VMware vSphere Client введите учетные данные администратора.
2. В левой панели нажмите на значок  .

   Откроется страница **Hosts and clusters**.
3. Если виртуальная машина включена, отключите ее. Для этого выберите виртуальную машину и в панели управления в раскрывающемся списке **Actions** выберите **Power** → **Power Off**.
4. В окне подтверждения нажмите на кнопку **Yes**. Дождитесь отключения машины.
5. В панели управления в раскрывающемся списке **Actions** выберите **Delete from Disk**.
6. В окне подтверждения нажмите на кнопку **Yes**.

Виртуальная машина с установленной программой Kaspersky Secure Mail Gateway будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины в консоли управления гипервизора Microsoft Hyper-V

Перед удалением программы требуется выполнить подготовительные действия.

► *Чтобы удалить виртуальную машину в консоли управления гипервизора Microsoft Hyper-V, выполните следующие действия:*

1. Запустите программу Hyper-V Manager.
2. В главном окне программы в списке виртуальных машин гипервизора в таблице **Virtual Machines** выберите виртуальную машину, которую вы хотите удалить.
3. Если виртуальная машина включена, отключите ее. Для этого по правой кнопке мыши откройте контекстное меню и выберите пункт **Turn Off**. Дождитесь отключения машины.
4. В контекстном меню виртуальной машины выберите пункт **Settings**.

   Откроется окно свойств виртуальной машины.
5. В блоке параметров **Hardware** выберите раздел **SCSI Controller** → **Hard Drive**.
6. Сохраните путь, указанный в поле **Virtual hard disk**, любым удобным для вас способом и закройте окно свойств виртуальной машины.

   По умолчанию после удаления виртуальной машины в консоли управления гипервизора файл виртуального жесткого диска не удаляется с сервера. Вам потребуется удалить его вручную.
7. В контекстном меню виртуальной машины выберите пункт **Delete**.
8. В окне подтверждения нажмите на кнопку **Delete**.
9. На физическом сервере гипервизора удалите вручную файл виртуального жесткого диска в папке, указанной в пункте 6.

Виртуальная машина с установленной программой Kaspersky Secure Mail Gateway будет удалена и перестанет отображаться в списке виртуальных машин.

Удаление виртуальной машины с помощью Microsoft SCVMM

Перед удалением программы требуется выполнить подготовительные действия.

► *Чтобы удалить виртуальную машину с помощью Microsoft SCVMM, выполните следующие действия:*

1. Запустите программу Virtual Machine Manager (VMM).
2. В левом нижнем углу окна выберите раздел **VMs and Services**.
3. В дереве в левой верхней панели выберите гипервизор, на котором была создана виртуальная машина.
4. В рабочей области выберите виртуальную машину, которую вы хотите удалить.
5. Если виртуальная машина включена, отключите ее. Для этого в панели инструментов нажмите на кнопку **Power Off**.
6. В окне подтверждения нажмите на кнопку **Yes**. Дождитесь отключения машины.
7. В панели инструментов нажмите на кнопку **Delete**.
8. В окне подтверждения нажмите на кнопку **Yes**.

Виртуальная машина с установленной программой Kaspersky Secure Mail Gateway будет удалена и перестанет отображаться в списке виртуальных машин.

kaspersky

Подготовка программы к работе

В этом разделе перечислены действия, которые вам нужно выполнить, чтобы подготовить программу к работе.

Интерфейс Kaspersky Secure Mail Gateway

Работа с Kaspersky Secure Mail Gateway осуществляется через веб-интерфейс.

Главное окно веб-интерфейса содержит следующие элементы:

- дерево консоли управления в левой части главного окна веб-интерфейса программы;
- рабочую область в правой части главного окна веб-интерфейса программы.

Дерево консоли управления Kaspersky Secure Mail Gateway

В дереве консоли управления Kaspersky Secure Mail Gateway отображаются следующие разделы:

- **Мониторинг**. Содержит графики и информационные панели, позволяющие отслеживать работу программы.
- **Правила**. Позволяет создавать и настраивать правила обработки сообщений.
- **Пользовательские списки**. Позволяет создавать и настраивать персональные пользовательские списки разрешенных и запрещенных адресов.
- **Узлы**. Позволяет управлять узлами кластера.
- **События**. Содержит информацию о событиях, обнаруженных в почтовом трафике, а также о системных событиях в работе программы.
- **Хранилище**. Содержит информацию о сообщениях, копии которых были помещены в Хранилище по результатам проверки модулями программы, а также фильтр поиска сообщений в Хранилище.
- **Очередь сообщений**. Содержит информацию об очереди сообщений почтового агента MTA и фильтр поиска сообщений в очереди.
- **Отчеты**. Позволяет формировать отчеты о работе программы, а также отправлять их по электронной почте.
- **Учетные записи**. Содержит информацию об учетных записях пользователей программы и правах доступа.
- **Параметры**. Содержит разделы **Общие**, **Персональные учетные записи**, **Внешние службы**, **Журналы и события**, **Мониторинг**, **Доступ к программе**, **Встроенный MTA**, в которых вы можете настраивать параметры программы.

Рабочая область окна веб-интерфейса Kaspersky Secure Mail Gateway

Рабочая область содержит информацию о разделах, которые вы выбираете в консоли управления, а также элементы управления, с помощью которых вы можете изменять параметры программы.

Для разделов, предусматривающих работу с параметрами Kaspersky Secure Mail Gateway, в рабочей области главного окна параметры сгруппированы в блоки параметров.

kaspersky

Подключение к веб-интерфейсу программы

Если вы подключаетесь к веб-интерфейсу впервые после установки программы, перед началом работы вам потребуется создать новый кластер (см. раздел "Создание нового кластера" на стр. 128).

► *Чтобы подключиться к веб-интерфейсу программы в режиме администратора:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или полное доменное имя (FQDN) Управляющего сервера>`

   Откроется страница авторизации веб-интерфейса с запросом имени и пароля пользователя.
2. В поле **Имя пользователя** введите имя учетной записи администратора.

   Для учетной записи Локального администратора укажите `Administrator`.
3. В поле **Пароль** введите пароль администратора.

   Пароль Локального администратора задается во время первоначальной настройки программы (см. раздел "Установка и первоначальная настройка программы" на стр. 67).

   Если вы введете неверный пароль пять раз, возможность авторизации будет заблокирована на пять минут.
4. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса программы. В левой панели меню отобразятся те разделы, на просмотр которых у администратора есть права (см. раздел "Работа с ролями и учетными записями пользователей" на стр. 139).

► *Чтобы подключиться к веб-интерфейсу программы в режиме пользователя:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или полное доменное имя (FQDN) Управляющего сервера>`

   Откроется страница авторизации веб-интерфейса с запросом имени и пароля пользователя.
2. Установите флажок **Войти с помощью доменных учетных данных**.
3. Нажмите на кнопку **Войти**.

Откроется главное окно веб-интерфейса программы. В левой панели меню отобразятся разделы с персональными списками адресов (см. раздел "Просмотр персональных списков разрешенных и запрещенных адресов" на стр. 126) и персональным Хранилищем при наличии у пользователя прав на просмотр этих разделов.

kaspersky

Состояние защиты почтового сервера

В разделе **Мониторинг** веб-интерфейса программы в правой части рабочей области отображается следующая информация о состоянии защиты почтового сервера:

- состояние работы модуля Анти-Спам, актуальность баз модуля Анти-Спам, количество сообщений в Анти-Спам карантине;
- состояние работы модуля Антивирус, актуальность баз модуля Антивирус;
- состояние соединения с сервером KATA, количество сообщений в KATA-карантине (если вы используете программу Kaspersky Anti Targeted Attack Platform);
- состояние подключения к Kaspersky Private Security Network;
- информация о последнем обновлении баз программы;
- состояние подключения к LDAP-серверам;
- срок действия лицензии и предупреждение о скором истечении срока действия лицензии, если он скоро истечет;
- информация о состоянии отправки и приема сообщений почтовым агентом MTA.

По умолчанию модули Анти-Спам и Антивирус включены, контентная фильтрация, проверка подлинности отправителей сообщений и защита KATA отключены.

Об участии в Kaspersky Security Network и использовании Kaspersky Private Security Network

Чтобы повысить эффективность защиты компьютера пользователя, Kaspersky Secure Mail Gateway использует данные, полученные от пользователей во всем мире. Для получения этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции Kaspersky Secure Mail Gateway на объекты, информация о которых еще не вошла в базы антивирусных программ, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках объектов, информация о которых еще не вошла в базы антивирусных программ, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний программы.

Во время участия в Kaspersky Security Network определенная статистика, полученная в результате работы Kaspersky Secure Mail Gateway, автоматически отправляется в "Лабораторию Касперского". Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Сбор, обработка и хранение персональных данных пользователя не производится. О данных, которые Kaspersky Secure Mail Gateway передает в Kaspersky Security Network, вы можете прочитать в Положении о KSN.

Участие в Kaspersky Security Network добровольное. Решение об участии в Kaspersky Security Network принимается на этапе установки Kaspersky Secure Mail Gateway, его можно изменить в любой момент.

Использование Kaspersky Security Network приводит к выходу программы из сертифицированного состояния. Рекомендуется использовать Kaspersky Private Security Network или отказаться от использования KSN. Для получения подробной информации см. Руководство администратора Kaspersky Private Security Network.

Если вы не хотите участвовать в KSN, вы можете использовать Kaspersky Private Security Network (далее также KPSN) – решение, позволяющее пользователям получать доступ к репутационным базам Kaspersky Security Network, а также другим статистическим данным, не отправляя данные в Kaspersky Security Network со своих компьютеров.

По вопросам приобретения программы Kaspersky Private Security Network вы можете связаться со специалистами компании-партнера "Лаборатории Касперского" в вашем регионе (http://www.kaspersky.ru/find_partner_office).

Настройка использования Kaspersky Private Security Network

► *Чтобы настроить использование KPSN, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **KSN/KPSN**.
2. Выберите закладку **Параметры KSN/KPSN**.
3. В раскрывающемся списке **Использование KSN/KPSN** выберите один из следующих вариантов:
   - **KPSN**, если вы хотите участвовать в KPSN.
   - **Не использовать**, если вы не хотите участвовать в KPSN.

   Если вы выбрали **KPSN**, в рабочей области отобразится блок параметров для добавления конфигурационного файла KPSN.
4. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
5. Выберите конфигурационный файл KPSN, который вы хотите добавить.

Конфигурационный файл KPSN должен быть в формате ZIP или PKCS7.

6. Нажмите на кнопку **Сохранить**.

Использование Kaspersky Private Security Network будет настроено.

kaspersky

Процедура приемки

После установки программы перед ее вводом в эксплуатацию проводится процедура приемки установленной программы, включающая проверку ее работоспособности и приведение конфигурации программы в соответствие с сертифицированной конфигурацией.

Перед запуском программа проверяет контрольные суммы модулей программы. Если при установке какого-либо модуля программы произошла ошибка, программа отображает сообщение об ошибке. Вам необходимо переустановить программу.

В этом разделе

Безопасное состояние программы

Программа находится в безопасном состоянии, если она работает в *сертифицированном режиме.* В сертифицированном режиме Kaspersky Secure Mail Gateway запрещен доступ в интернет и соединение с серверами, расположенными за пределами IT-инфраструктуры вашей организации. Параметры программы находятся в рамках допустимых значений, приведенных в приложении к данному документу.

Вы можете выбрать сертифицированный режим работы Kaspersky Secure Mail Gateway при развертывании образа виртуальной машины Kaspersky Secure Mail Gateway.

В сертифицированном режиме параметры компонентов программы, которые требуют доступ в интернет, по умолчанию принимают следующие значения:

- Использование KSN отключено.
- SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений отключены, соединение с DNS-серверами запрещено.
- Параметр Enforced Anti-Spam Updates отключен в параметрах модуля Анти-Спам.
- В качестве источника обновлений баз программы используется Kaspersky Security Center или локальный источник обновлений баз Kaspersky Secure Mail Gateway.

Проверка работоспособности. Eicar

Перед началом проверки убедитесь, что выполнены следующие условия:

- Программа готова к работе.
- Программа находится в безопасном состоянии.

kaspersky

Проверка работы программы с использованием тестового файла EICAR

Вы можете проверить, как работает защита интернет-трафика, антивирусная защита файлов и проверка на вирусы с помощью тестового файла EICAR.

Не забудьте возобновить антивирусную защиту интернет-трафика и антивирусную защиту файлов после завершения работы с тестовым файлом EICAR.

► *Чтобы проверить защиту интернет-трафика с использованием тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
2. Сохраните тестовый файл EICAR.

   Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы по запрашиваемому веб-адресу и заблокирует сохранение объекта.
3. Если требуется, используйте виды тестового файла EICAR.

► *Чтобы проверить антивирусную защиту файлов с использованием тестового файла EICAR или его вида, выполните следующие действия:*

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

   Когда защита приостановлена, не рекомендуется подключать устройство к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб этому устройству.
2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
3. Сохраните тестовый файл EICAR.
4. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.
5. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.
6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов.
7. Запустите сохраненный файл.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.

► *Чтобы проверить, как работает поиск вирусов с использованием тестового файла EICAR или его вида, выполните следующие действия*:

1. Приостановите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

Когда защита приостановлена, не рекомендуется подключать устройство к локальным сетям и использовать съемные носители информации, чтобы вредоносные программы не смогли нанести ущерб этому устройству.

2. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
3. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.
4. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.
5. Запустите проверку сохраненного файла.

   Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.
6. Возобновите антивирусную защиту интернет-трафика и антивирусную защиту файлов.

Проверка антивирусной защиты сообщений с использованием тестового файла EICAR

Вы можете проверить работу антивирусной защиты сообщений с помощью тестового файла EICAR или одного из видов тестового файла EICAR.

► *Чтобы проверить антивирусную защиту сообщений с использованием тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
2. Сохраните тестовый файл EICAR.
3. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Secure Mail Gateway.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

► *Чтобы проверить антивирусную защиту сообщений с использованием одного из видов тестового файла EICAR, выполните следующие действия:*

1. Загрузите тестовый файл EICAR с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.
2. Сохраните тестовый файл EICAR.
3. Добавьте в начало строки тестового файла EICAR один из префиксов. Для этого вы можете использовать любой текстовый или гипертекстовый редактор.
4. Сохраните полученный файл под именем, соответствующим виду файла EICAR.

   Например, вы можете добавить префикс DELE-. Сохраните полученный файл под именем eicar_dele.com.
5. Отправьте почтовое сообщение с сохраненным тестовым файлом EICAR на компьютер с установленной программой Kaspersky Secure Mail Gateway.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и заблокирует сохранение объекта.

6. Запустите сохраненный файл.

Kaspersky Secure Mail Gateway сообщит вам об обнаружении угрозы и выполнит над ней действие, настроенное в параметрах проверки.

Проверка работоспособности модуля Анти-Спам

Вы можете проверить работоспособность модуля Анти-Спам с помощью образца спама.

В качестве образца спама используется строка GTUBE (Generic Test for Unsolicited Bulk Email): XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X.

► *Чтобы проверить работоспособность модуля Анти-Спам, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Спам**.
3. Включите модуль Анти-Спам с помощью переключателя **Использовать Анти-Спам**.
4. В левой панели выберите раздел **Правила**.
5. Выберите правило, которое вы хотите использовать для проверки работоспособности модуля Анти-Спам.

   Откроется окно **Просмотреть правило**.
6. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
7. В левой панели выберите раздел **Анти-Спам**.
8. Включите проверку модулем Анти-Спам сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.
9. В блоке параметров **Если обнаружен спам** установите флажок **Поместить копию в Хранилище**..
10. Запустите утилиту SwithMail.
11. Укажите адрес отправителя, назначения, а также адрес программы.
12. Откройте закладку Email Content.
13. В поле Email Subject введите gtube.
14. В поле Email Body введите строку GTUBE.
15. Нажмите на кнопку Test Settings.

    Тестовое спам-сообщение будет отправлено.
16. Перейдите в почтовый ящик пользователя, адрес электронной почты которого вы указали в качестве адреса назначения.
17. Убедитесь, что отправленное вами письмо было доставлено с меткой [Spam].
18. В окне веб-интерфейса программы выберите раздел **Хранилище**.

19. Убедитесь, что в таблице объектов Хранилища появилась запись об отправленном тестовом спам-сообщении.

    Если запись не появилась, проверьте, правильно ли вы настроили фильтрацию сообщений в Хранилище.

kaspersky

Мониторинг работы программы

Вы можете осуществлять мониторинг работы программы с помощью графиков и информационных панелей. Вы можете фильтровать данные мониторинга (см. раздел "Фильтрация данных мониторинга" на стр. 97) по интервалу времени и узлам кластера.

В разделе **Мониторинг** веб-интерфейса программы доступна следующая информация:

1. **Работоспособность системы**. Диаграмма ошибок в работе кластера. По ссылке **Перейти в раздел Узлы** вы можете перейти в раздел **Узлы** и посмотреть более подробные сведения о работоспособности каждого узла кластера.
2. **Обработано**. График, показывающий статистику действий программы, примененных ко всем обработанным сообщениям электронной почты:
   - **Удалены вложения**.
   - **Удалено**.
   - **Вылечено**.
   - **Помещено в Карантин**.
   - **Отклонено**.
   - **Пропущено**.

   С помощью кнопок **Размер** и **Количество** вы можете переключать отображение на графике суммарного размера или количества всех обработанных сообщений соответственно.
3. **Обнаружено**. График количества обнаруженных объектов, сгруппированных по модулям защиты:
   - **Анти-Фишинг**.
   - **Анти-Спам**.
   - **Антивирус**.
   - **Контентная фильтрация**.
   - **Проверка подлинности**.
   - **Проверка ссылок**.
   - **KATA**.

     Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

   > Если в одном сообщении было обнаружено несколько объектов одним модулем защиты, то в статистике для этого модуля защиты считается только один объект. Если в одном сообщении было обнаружено несколько объектов разными модулями защиты, то в статистике считается по одному объекту для каждого модуля защиты.

   По ссылке в правом нижнем углу информационной панели вы можете перейти в раздел **События**, чтобы просмотреть связанные события с информацией об обнаружениях за выбранный период (см. раздел "Фильтрация данных мониторинга" на стр. 97).
4. Графики, которые показывают количество сообщений, проверенных определенным модулем и сгруппированных по результату проверки:

- **Антивирус**.
- **Анти-Спам**.
- **Анти-Фишинг**.
- **Контентная фильтрация**.
- **Проверка ссылок**.
- **Проверка подлинности**.

На всех графиках со статистикой по модулям защиты отображаются следующие статусы проверки:

- **Обнаружено** – в сообщении обнаружен объект, удовлетворяющий критериям применения правила.
- **Не обнаружено** – сообщение проверено и не содержит угроз и других объектов.
- **Документ с макросом** – в сообщении есть вложение, содержащее документ с макросом.

  Применимо только к графику **Антивирус**.
- **Помещено в Карантин** – сообщение помещено в Анти-Спам карантин.

  Применимо только к графику **Анти-Спам**.
- **Не обработано** – группа статусов, присваиваемых сообщению, если оно не было проверено по одной из следующих причин:
  - **Зашифровано** – не удалось проверить объект из-за того, что он зашифрован.

    Применимо только к графику **Антивирус**.
  - **Ошибка** – при проверке сообщения произошла ошибка.
  - **Ошибка баз** – не удалось проверить сообщение из-за того, что базы программы не загружены (см. раздел "Мониторинг состояния баз программы" на стр. 219).
  - **Ограничения лицензирования** – не удалось проверить сообщение из-за ограничений, связанных с лицензированием программы (см. раздел "Мониторинг статуса лицензионного ключа" на стр. 43) (например, истек срок действия лицензионного ключа).
  - **Отключено в параметрах** – группа статусов, присваиваемых сообщению, если оно не было проверено согласно одному из следующих параметров программы, заданных администратором:
    - **Список разрешенных адресов** – сообщение доставлено без проверки, т.к. адрес отправителя сообщения находится в глобальном списке разрешенных адресов (см. раздел "Списки разрешенных и запрещенных адресов" на стр. 123).
    - **Список запрещенных адресов** – сообщение отклонено без проверки, т.к. адрес отправителя сообщения находится в глобальном списке запрещенных адресов (см. раздел "Списки разрешенных и запрещенных адресов" на стр. 123).
    - **Превышен уровень вложенности** – превышен максимальный уровень вложенности архивов, заданный в общих параметрах защиты (см. раздел "Общие параметры защиты" на стр. 195).

      Применимо только к графику **Антивирус**.
    - **Персональный список разрешенных адресов** – сообщение не было проверено модулем Анти-Спам, т.к. адрес отправителя находится в персональном списке разрешенных адресов (см. раздел "Формирование персональных списков" на стр. 127) получателя.

      Применимо только к графику **Анти-Спам**.

- **Персональный список запрещенных адресов** – адрес отправителя находится в персональном списке запрещенных адресов получателя. К сообщению применено действие, заданное в параметрах персональных списков (см. раздел "Настройка параметров персональных списков" на стр. 125).

  При подсчете не учитываются сообщения, помещенные в Хранилище согласно параметрам персональных списков. Такие сообщения попадают в статистику по другим статусам в соответствии с результатом проверки.

- **Локальная политика** – сообщение было отправлено с локального IP-адреса.

  Применимо только к графику **Проверка подлинности**.

- **Отключено в параметрах защиты** – модуль отключен в общих параметрах защиты или в правиле обработки сообщений.

- **Обработано ранее другим модулем** – сообщение не было проверено данным модулем, т.к. ранее была выполнена проверка другим модулем защиты и к сообщению уже применено действие **Отклонить** или **Удалить сообщение** (при этом копия сообщения не была помещена в Хранилище).

5. **Последние угрозы**. Таблица с информацией о недавних обнаруженных угрозах:

   - **Время** – время обнаружения угрозы.
   - **Название угрозы** – название угрозы, обнаруженной в объекте.
   - **Результат** – действие, выполненное с объектом.

   > Отображаются сведения, доступные в программе на текущий момент. Критерии фильтрации по времени (см. раздел "Фильтрация данных мониторинга" на стр. 97) не применяются.

6. **Сообщения**. График, который показывает объем исходящего и входящего почтового трафика, обработанного программой.

   > При подсчете исходящих сообщений не учитываются уведомления, отправляемые программой, и сообщения со статусами проверки **Удалено**, **Отклонено** и **Помещено в Карантин**.

   С помощью кнопок **Размер** и **Количество** вы можете переключать отображение на графике суммарного размера или количества исходящих и входящих сообщений соответственно.

7. **Топ сработавших правил**. Таблица с информацией о правилах, которые наиболее часто применялись при обработке сообщений:

   - **Название правила** – название примененного правила, заданное администратором.
   - **Количество** – количество срабатываний правила.

   > Если правило было удалено администратором, то оно не отображается на этой информационной панели.

По умолчанию отображаются не все информационные панели. Вы можете создать новую схему расположения (см. раздел "Создание новой схемы расположения графиков" на стр. 95) и добавить на нее необходимые панели, а затем переключаться между доступными схемами (см. раздел "Выбор схемы расположения графиков из списка" на стр. 96).

kaspersky

В этом разделе

Создание новой схемы расположения графиков

После установки программы в разделе **Мониторинг** отображается только схема расположения по умолчанию. Вы можете создать новую схему и настроить отображение информационных панелей на ней.

► *Чтобы создать новую схему расположения графиков:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В верхней части окна нажмите на кнопку  .
3. В раскрывшемся списке выберите **Новая схема**.

   Отобразится набор графиков по умолчанию.
4. Если вы хотите изменить стандартное название схемы, выполните следующие действия:
   a. В верхней части рабочей области рядом с названием **Новая схема #** нажмите на значок  .
   b. В открывшемся окне в поле **Название схемы расположения графиков** введите новое название.
   c. Нажмите на кнопку **Сохранить**.
5. Если вы хотите добавить графики на схему, выполните следующие действия:
   a. Нажмите на кнопку **Добавить график**.

      Откроется окно **Добавить график**.
   b. Установите флажки рядом с названиями тех графиков, которые вы хотите добавить на схему расположения графиков.
   c. Нажмите на кнопку **Добавить**.
6. Если вы хотите переместить график на схеме, перетащите график на другое место схемы, нажав и удерживая левую клавишу мыши на верхней части графика.
7. Если вы хотите удалить график со схемы, нажмите на значок  в правом верхнем углу панели.
8. Если вы хотите изменить масштаб графика, нажмите на значок  в правом верхнем углу панели и в раскрывшемся списке выберите нужное значение.
9. Если вы хотите отключить отображение какой-либо категории данных на графике, нажмите на цветовой индикатор слева от этой категории (например,  для объектов со статусом **Не обнаружено**).

10. Если требуется, измените способ отображения информации (гистограмма или график) с помощью переключателя  в правом верхнем углу панели.
11. Нажмите на кнопку **Сохранить**.

Новая схема будет добавлена в список схем расположения графиков в разделе **Мониторинг**. Вы сможете выбрать ее из списка доступных схем (см. раздел "Выбор схемы расположения графиков из списка" на стр. 96).

Изменение схемы расположения графиков

► *Чтобы изменить схему расположения графиков:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите изменить.
3. Нажмите на кнопку  и в раскрывшемся списке выберите **Изменить схему**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Схема расположения графиков будет изменена.

Удаление схемы расположения графиков

► *Чтобы удалить схему расположения графиков:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите удалить.
3. Нажмите на кнопку  и в раскрывшемся списке выберите **Удалить схему**.

Схема расположения графиков будет удалена.

Выбор схемы расположения графиков из списка

► *Чтобы выбрать схему расположения графиков из списка доступных:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. В правом верхнем углу рабочей области в правом раскрывающемся списке выберите схему расположения графиков, которую вы хотите открыть.

Выбранная схема отобразится в рабочей области.

Фильтрация данных мониторинга

► *Чтобы отфильтровать данные, отображаемые на графиках:*

1. В окне веб-интерфейса программы выберите раздел **Мониторинг**.
2. Если вы хотите отфильтровать данные по интервалу времени, в правом верхнем углу рабочей области в левом раскрывающемся списке выберите один из следующих вариантов:
   - **Прошедший час**.
   - **Прошедшие сутки**.
   - **Прошедшая неделя**.
   - **Прошедший месяц**.
   - **Прошедший год**.

   По умолчанию отображаются данные за последний час.
3. Если вы хотите отфильтровать данные по узлам кластера, в среднем раскрывающемся списке выберите IP-адрес нужного узла.

   По умолчанию отображаются данные обо всех узлах.

Данные, отображаемые на графиках, будут отфильтрованы по заданным критериям.

kaspersky

Работа с правилами обработки сообщений

Правило обработки сообщений (далее также "правило") – заданное множество пар адресов отправителей и получателей, сообщения электронной почты которых Kaspersky Secure Mail Gateway обрабатывает в соответствии с одними и теми же значениями параметров. Принадлежность сообщения электронной почты к правилу определяется наличием в этом правиле как адреса отправителя, так и адреса получателя.

По умолчанию в программе предусмотрены следующие предустановленные правила обработки сообщений:

- **AllowList** – обработка сообщений из глобального списка разрешенных адресов.
- **DenyList** – обработка сообщений из глобального списка запрещенных адресов.
- **Default** – обработка сообщений по предустановленным "Лабораторией Касперского" параметрам.

> Правила **AllowList** и **DenyList** по умолчанию отключены.

Обрабатывая сообщение электронной почты, Kaspersky Secure Mail Gateway применяет правила согласно их приоритету – в порядке расположения в таблице правил сверху вниз. Если комбинация адресов *отправитель-получатель* не совпадает, программа переходит к следующему правилу. Как только комбинация адресов отправитель-получатель найдена в каком-либо правиле, к сообщению применяются параметры обработки, заданные в этом правиле, и поиск совпадения завершается.

Если ни одно правило не содержит комбинацию адресов отправитель-получатель, сообщение обрабатывается в соответствии с параметрами, заданными для предустановленного правила **Default**.

Для каждого правила вы можете задать собственные критерии обработки сообщений электронной почты и выбрать действие, применяемое к сообщениям.

Рекомендуется устанавливать действие **Отклонить**, только если программа Kaspersky Secure Mail Gateway встроена в почтовую инфраструктуру напрямую, то есть выступает в роли пограничного шлюза. Если программа встроена за сторонним пограничным шлюзом, то есть выступает в роли внутреннего шлюза, то в случае применения действия **Отклонить** пограничный шлюз будет формировать уведомления о недоставке (DSN, Delivery status notification). Рассылка таких уведомлений на несуществующие адреса электронной почты может привести к снижению репутации пограничного шлюза в сети Интернет.

kaspersky

В этом разделе

Просмотр таблицы правил

► *Чтобы просмотреть таблицу правил,*

в окне веб-интерфейса программы выберите раздел **Правила**.

В таблице отображается следующая информация о правилах:

- **Приоритет**.

  Номер, соответствующий приоритету, задает последовательность применения правил. Правила применяются в порядке их расположения в таблице сверху вниз, то есть от наивысшего приоритета к низшему.

- **Название правила**.

  Название правила, заданное пользователем.

- **Статус**.

  Переключатель для включения и отключения правила.

- **Режим**.

  Правило может работать в одном из следующих режимов:

  -  – **Использовать параметры модулей проверки**.
  -  – **Отклонять без проверки**.
  -  – **Удалять без уведомления отправителя**.
  -  – **Пропускать без проверки**.

- **Описание**.

  Любая дополнительная информация о правиле, указанная пользователем.

По ссылке **Уведомления об обнаружениях** вы можете настроить общие параметры почтовых уведомлений об обнаружениях (см. раздел "Настройка уведомлений о срабатывании правил обработки

сообщений" на стр. 264), применимые ко всем правилам. После этого требуется включить уведомления для каждого правила (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 117), о срабатывании которого вы хотите получать сообщения от программы.

Настройка отображения таблицы правил

► *Чтобы настроить отображение таблицы правил, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Нажмите на кнопку  .

   Откроется окно **Настроить таблицу**.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы правил будет настроено.

Сценарий настройки правил обработки сообщений

Вы можете изменить общие параметры защиты (на стр. 195), применяемые ко всем правилам обработки сообщений, в разделе **Параметры** → **Общие**.

a. **Создание правила (см. раздел "Создание правила обработки сообщений" на стр. 102)**

   При создании правила необходимо задать адреса отправителей и получателей, сообщения которых будут обрабатываться согласно параметрам этого правила, а также режим обработки сообщений. Остальные общие параметры правила являются опциональными.

b. **Антивирусная защита сообщений (см. раздел "Настройка антивирусной защиты" на стр. 104)**

   Kaspersky Secure Mail Gateway проверяет сообщения электронной почты на вирусы и другие программы, представляющие угрозу, с помощью модуля Антивирус.

   Вы можете включить или отключить антивирусную проверку сообщений для правила. Если в правиле включена антивирусная проверка, то вы можете настроить параметры проверки в зависимости от типа объекта:

   - зараженные и возможно зараженные объекты, а также легальные программы, которые могут быть использованы злоумышленниками;
   - объекты, во время проверки которых возникли ошибки;
   - зашифрованные объекты;
   - вложения с макросами.

c. **Проверка ссылок (см. раздел "Настройка проверки ссылок" на стр. 107)**

   Kaspersky Secure Mail Gateway проверяет, являются ли ссылки в тексте сообщения вредоносными, т.е. ведущими на веб-ресурсы, которые распространяют вредоносное ПО. Вы также можете

включить обнаружение рекламных ссылок и ссылок, относящихся к легальным программам (см. раздел "Настройка параметров проверки ссылок" на стр. 205).

d. **Защита сообщений от спама (см. раздел "Настройка защиты от спама" на стр. 108)**

Kaspersky Secure Mail Gateway фильтрует сообщения, проходящие через почтовый сервер, от нежелательной почты (спама) с помощью модуля Анти-Спам.

Вы можете включить или отключить защиту от спама для правила. Если в правиле включена защита от спама, то вы можете настроить параметры проверки в зависимости от типа объекта:

- спам;
- предполагаемый спам;
- массовая рассылка.

e. **Защита сообщений от фишинга (см. раздел "Настройка защиты от фишинга" на стр. 110)**

Kaspersky Secure Mail Gateway фильтрует сообщения, проходящие через почтовый сервер, от фишинга с помощью модуля Анти-Фишинг.

Вы можете включить или отключить защиту от фишинга для правила.

f. **Контентная фильтрация сообщений (см. раздел "Настройка контентной фильтрации" на стр. 111)**

Kaspersky Secure Mail Gateway выполняет контентную фильтрацию сообщений, проходящих через почтовый сервер.

Вы можете включить или отключить контентную фильтрацию для правила. Если в правиле включена контентная фильтрация, вы можете ограничить пересылку почтовым сервером сообщений по следующим критериям:

- размер сообщения;
- маска имен вложенных файлов;
- формат вложенных файлов.

g. **Проверка подлинности отправителей сообщений (на стр. 114)**

Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры вашей организации от спама и фишинга.

Kaspersky Secure Mail Gateway использует следующие технологии проверки подлинности отправителей сообщений:

- SPF-проверку (Sender Policy Framework).
- DKIM-проверку (DomainKeys Identified Mail).
- DMARC-проверку (Domain-based Message Authentication, Reporting and Conformance).

h. **Уведомления о результатах проверки сообщений (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 117)**

Вы можете настроить отправку почтовых уведомлений о событиях проверки сообщений на адреса из заданного общего списка, отправителю, получателям сообщения или другим адресатам.

i. **Предупреждения о небезопасных сообщениях (см. раздел "Добавление предупреждения о небезопасном сообщении" на стр. 119)**

Вы можете настроить шаблон предупреждения, текст которого будет добавляться в тело сообщения, имеющего один из следующих статусов проверки:

- *Зашифровано*;
- *Заражено*;
- *Ошибка*;
- *Фишинг*;
- *Проверка ссылок*.

j. **Примечания к сообщениям (см. раздел "Добавление примечания к событиям проверки сообщений" на стр. 119)**

Примечание к сообщениям (далее также "примечание") – это текст, который программа может добавлять в конце сообщения электронной почты.

Вы можете включить или отключить использование примечаний для одного или нескольких правил обработки сообщений, а также настроить шаблоны примечаний.

k. **Защита KATA (см. раздел "Настройка защиты KATA" на стр. 120)**

Kaspersky Secure Mail Gateway может интегрироваться с Kaspersky Anti Targeted Attack Platform и отправлять сообщения для проверки на сервер KATA.

Вы можете включить или отключить защиту KATA для правила. Если в правиле включена защита KATA, то вы можете выбрать действие для сообщений, в которых обнаружены объекты, указать, должна ли программа помещать копию сообщений в Хранилище, а также настроить метку в теме сообщений.

Создание правила обработки сообщений

► *Чтобы создать правило обработки сообщений, выполните следующие действия:*

1. В главном окне веб-интерфейса программы в дереве консоли управления выберите раздел **Правила**.
2. В верхней части рабочей области нажмите на кнопку **Создать**.

   Откроется новое правило обработки сообщений.
3. В левой панели выберите раздел **Общие**.
4. В поле **Название правила** введите название нового правила.

   Название правила должно быть уникальным в списке правил Kaspersky Secure Mail Gateway.
5. В поле **Описание** введите описание правила.
6. В блоке параметров **Режим** выберите один из следующих вариантов обработки сообщений, соответствующих критериям этого правила:

   - **Использовать параметры модулей проверки** – использовать параметры модулей Антивирус, Анти-Спам, Анти-Фишинг и параметры контентной фильтрации.

     В левой панели станут доступны разделы, в которых вы можете настроить параметры модулей, применяемые в этом правиле.
   - **Отклонять без проверки** – отклонять сообщения, не выполняя их проверку модулями Антивирус, Анти-Спам, Анти-Фишинг и не применяя к ним параметры контентной фильтрации.
   - **Удалять без уведомления отправителя** – удалять сообщения, не уведомляя отправителя о том, что сообщение не было доставлено.

- **Пропускать без проверки** – доставлять сообщения, не выполняя их проверку.

7. Если вы хотите изменить приоритет создаваемого правила, в блоке **Приоритет правила** задайте позицию создаваемого правила в таблице правил.

   По умолчанию правилу присваивается наивысший приоритет из всех ранее созданных правил.

8. В блоке параметров **Адрес отправителя** укажите отправителей сообщения, для которых должно применяться это правило. Для этого выберите одну из следующих закладок:

   - **Email**

   В поле ввода укажите адрес электронной почты и нажмите на клавишу **ENTER**.

   Адреса электронной почты вводятся по одному. Повторите указанные действия для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "re:".

   Регулярные выражения нечувствительны к регистру.

   - **IP**

   В поле ввода укажите IP-адрес отправителя сообщений и нажмите на клавишу **ENTER**.

   IP-адреса вводятся по одному. Повторите указанные действия для всех добавляемых IP-адресов.

   Вы можете ввести IPv4-адрес (например, 192.0.0.1), IPv4-адрес подсети с маской (например, 192.0.0.0/16), IPv6-адрес (например, 2607:f0d0:1002:51::4) или IPv6-адрес подсети с маской (например, fc00::/7).

   - **LDAP: DN**

   В поле ввода укажите учетную запись LDAP и нажмите на клавишу **ENTER**.

   Учетные записи вводятся по одной. Повторите указанные действия для всех добавляемых учетных записей.
   Для того, чтобы правило применялось, необходимо указать хотя бы одного отправителя.

9. В блоке параметров **Адрес получателя** укажите получателей сообщения, для которых должно применяться это правило. Для этого выберите одну из следующих закладок:

   - **Email**

   В поле ввода укажите адрес электронной почты и нажмите на клавишу **ENTER**.

   Адреса электронной почты вводятся по одному. Повторите указанные действия для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "re:".

Регулярные выражения нечувствительны к регистру.

- **LDAP: DN**

В поле ввода укажите учетную запись LDAP и нажмите на клавишу **ENTER**.

Учетные записи вводятся по одной. Повторите указанные действия для всех добавляемых учетных записей.
Для того, чтобы правило применялось, необходимо указать хотя бы одного получателя.

10. В правом нижнем углу нажмите на кнопку **Сохранить**.

Правило будет создано и добавлено в таблицу правил в разделе **Правила**.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, требуется включить правило (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122). По умолчанию новое правило отключено и не используется в работе программы.

Настройка антивирусной защиты

Перед тем как настроить параметры антивирусной защиты в правиле обработки сообщений, убедитесь, что модуль Антивирус включен (см. раздел "Настройка параметров модуля Антивирус" на стр. 204) в общих параметрах защиты.

► *Чтобы настроить параметры антивирусной защиты в правиле обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры антивирусной защиты.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Антивирус**.
5. Включите или отключите проверку модулем Антивирус сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию антивирусная защита сообщений включена.
6. Если на предыдущем шаге вы включили антивирусную проверку, настройте параметры модуля Антивирус, применяемые по результатам проверки к следующим типам объектов:

   - Зараженные и возможно зараженные объекты, а также легальные программы, которые могут быть использованы злоумышленниками.

7. В блоке параметров **Если обнаружен зараженный объект** в раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:

   - **Пропустить**.
   - **Вылечить**.
   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Вылечить**.

8. Если на предыдущем шаге вы выбрали действие **Вылечить**, в раскрывающемся списке **Если вылечить не удалось** выберите одно из следующих действий над зараженными сообщениями, вылечить которые не удалось:

   - **Удалить вложение**.
   - **Удалить сообщение**.
   - **Отклонить**.

   По умолчанию выбрано действие **Удалить вложение**.

9. Если вы хотите чтобы по результатам антивирусной проверки сообщения с обнаруженными объектами автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок установлен.

10. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы зараженных и вылеченных сообщений, укажите текст меток в полях ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию добавлены метки *[Infected]* и *[Cured]*.

    - Объекты, во время проверки которых произошли ошибки.

11. В раскрывающемся списке **Если обнаружены ошибки проверки модулем Антивирус** выберите действие, применяемое к сообщениям, при проверке которых произошли ошибки:

    - **Пропустить**.
    - **Удалить вложение**.
    - **Удалить сообщение**.
    - **Отклонить**.

    По умолчанию выбрано действие **Пропустить**.

12. Если вы хотите чтобы сообщения, при проверке которых произошли ошибки, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок снят.

13. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы сообщений, при проверке которых произошли ошибки, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

    - Зашифрованные объекты.

14. В раскрывающемся списке **Если обнаружен зашифрованный объект** выберите действие, применяемое к сообщениям, содержащим зашифрованные объекты:

- **Пропустить**.
- **Удалить вложение**.
- **Удалить сообщение**.
- **Отклонить**.

По умолчанию выбрано действие **Пропустить**.

15. Если вы хотите чтобы по результатам проверки сообщения с зашифрованными объектами автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок снят.

16. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы сообщений, содержащих зашифрованные объекты, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

- Вложения с макросами.

17. В блоке параметров **Если обнаружен макрос** установите флажок **Обрабатывать вложения с макросами** если вы хотите, чтобы программа обрабатывала вложения с макросами.
18. В раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:

- **Пропустить**.
- **Удалить вложение**.
- **Удалить сообщение**.
- **Отклонить**.

По умолчанию выбрано действие **Удалить вложение**.

19. Если вы хотите чтобы по результатам проверки сообщения, содержащие вложения с макросами, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок снят.

20. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы сообщений, содержащих вложения с макросами, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию добавлена метка *[Attachments with Macros]*.

21. Если требуется, настройте список исключений из проверки. Для этого в блоке параметров **Исключения из проверки** выполните следующие действия:

    a. Если вы хотите исключить из антивирусной проверки архивы, установите флажок **Не проверять архивы**.

    b. Если вы хотите исключить из антивирусной проверки вложенные в сообщение объекты с определенными именами, в поле **Не проверять вложения по маскам имени** укажите маску имени и нажмите на клавишу **ENTER**.

       Вводите маски по одной. Повторите указанные действия для каждой добавляемой маски.

       > Маски могут содержать любые символы.

22. Нажмите на кнопку **Сохранить**.

Антивирусная защита будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что антивирусная проверка сообщений для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Настройка проверки ссылок

Перед тем как настроить параметры проверки ссылок в правиле обработки сообщений, убедитесь, что проверка ссылок включена (см. раздел "Настройка параметров проверки ссылок" на стр. 205) в общих параметрах защиты.

► *Чтобы настроить параметры проверки ссылок в правиле обработки сообщений:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры антивирусной защиты.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Проверка ссылок**.
5. Включите или отключите проверку ссылок в сообщениях, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию проверка ссылок включена.
6. Если на предыдущем шаге вы включили проверку ссылок, настройте параметры, применяемые по результатам проверки к вредоносным или рекламным ссылкам, а также к ссылкам, относящимся к легальным программам:
   a. В раскрывающемся списке **Действие** выберите действие, которое будет применяться к сообщениям:
      - **Удалить сообщение**.
      - **Отклонить**.
      - **Пропустить**.

      По умолчанию выбрано действие **Отклонить**.
   b. Если вы хотите чтобы по результатам проверки сообщения с обнаруженными объектами автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

      По умолчанию флажок установлен.

c. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы сообщений, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию добавлена метка *[Malicious|Adware|Legitimate links]*.

7. Нажмите на кнопку **Сохранить**.

Настройка защиты от спама

Перед тем как настроить параметры защитыот спама в правиле обработки сообщений, убедитесь, что модуль Анти-Спам включен (см. раздел "Настройка параметров модуля Анти-Спам" на стр. 206) в общих параметрах защиты.

► *Чтобы настроить параметры защиты от спама в правиле обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры защиты от спама.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Анти-Спам**.
5. Включите или отключите проверку модулем Анти-Спам сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита сообщений от спама включена.
6. Если на предыдущем шаге вы включили защиту от спама, настройте параметры модуля Анти-Спам, применяемые по результатам проверки к следующим типам объектов:
   - Спам.
7. В блоке параметров **Если обнаружен спам** выберите одно из следующих действий над сообщениями, содержащими спам:
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Пропустить**.
8. Если вы хотите чтобы по результатам проверки сообщения, признанные спамом, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок снят.
9. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, содержащих спам, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию добавлена метка *[Spam]*.

- Предполагаемый спам.

10. В блоке параметров **Если обнаружен предполагаемый спам** выберите одно из следующих действий над сообщениями, содержащими предполагаемый спам:

    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Пропустить**.

11. Если вы хотите чтобы по результатам проверки сообщения, содержащие предполагаемый спам, помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок снят.

12. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, содержащих предполагаемый спам, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию добавлена метка *[Probable spam]*.

    - Массовая рассылка.

13. В блоке параметров **Если обнаружена массовая рассылка** выберите одно из следующих действий над сообщениями, являющимися массовой рассылкой:

    - **Удалить сообщение**.
    - **Отклонить**.
    - **Пропустить**.

    По умолчанию выбрано действие **Пропустить**.

14. Если вы хотите чтобы по результатам проверки сообщения, признанные массовой рассылкой, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок снят.

15. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, являющихся массовой рассылкой, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию добавлена метка *[MASSMAIL]*.

16. В блоке параметров **Дополнительные параметры** установите флажки рядом с названиями параметров, которые вы хотите включить:

    a. **Использовать технологии обработки графических изображений**, если вы хотите использовать технологию GSG, позволяющую идентифицировать изображения, содержащие текст, чтобы затем определить, является ли текст спамом. Текст распознается вне зависимости от того, был ли он модифицирован, повернут на изображении, «зашумлен» или подвергнут любой другой обработке, скрывающей назначение отправленного изображения.

    b. **Защита от Юникод-спуфинга**, если вы хотите включить защиту от Юникод-спуфинга. В случае обнаружения Юникод-спуфинга сообщение считается спамом. Программа добавляет метку `unicode_spoof` к заголовку сообщения `X-KSMG-AntiSpam-Method`.

    > Программа проверяет наличие Юникод-спуфинга только в заголовках Mail From SMTP-конверта, а также в заголовках сообщения From, Sender, Reply-To.

17. Нажмите на кнопку **Сохранить**.

Защита от спама будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что защита от спама для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Настройка защиты от фишинга

Перед тем как настроить параметры защиты от фишинга в правиле обработки сообщений, убедитесь, что модуль Анти-Фишинг включен (см. раздел "Настройка параметров модуля Анти-Фишинг" на стр. 208) в общих параметрах защиты.

► *Чтобы настроить параметры защиты от фишинга в правиле обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры защиты от фишинга.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Анти-Фишинг**.
5. Включите или отключите проверку модулем Анти-Фишинг сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита сообщений от фишинга включена.
6. Если на предыдущем шаге вы включили защиту от фишинга, в раскрывающемся списке выберите одно из следующих действий над сообщениями, содержащими фишинг:
   - **Удалить сообщение**.
   - **Отклонить**.
   - **Пропустить**.

   По умолчанию выбрано действие **Отклонить**.
7. Если вы хотите чтобы по результатам проверки сообщения, содержащие фишинг, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок снят.

8. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, содержащих фишинг, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию добавлена метка *[Phishing]*.

9. Нажмите на кнопку **Сохранить**.

Защита от фишинга будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что защита от фишинга для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Настройка контентной фильтрации

Перед тем как настроить параметры контентной фильтрации в правиле обработки сообщений, убедитесь, что контентная фильтрация включена (см. раздел "Настройка параметров контентной фильтрации" на стр. 208) в общих параметрах защиты.

► *Чтобы настроить параметры контентной фильтрации в правиле обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить параметры контентной фильтрации.

   Откроется окно **Просмотреть правило**.

3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Контентная фильтрация**.
5. Включите или отключите контентную фильтрацию сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию контентная фильтрация сообщений отключена.

6. Если на предыдущем шаге вы включили контентную фильтрацию, настройте параметры фильтрации по следующим критериям:

   - по размеру сообщений;

7. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты определенного размера, в блоке параметров **Если превышен допустимый размер сообщения** в раскрывающемся списке выберите действие, которое будет применяться к сообщениям:

   - **Пропустить**.

- **Удалить сообщение**.
- **Отклонить**.

По умолчанию выбрано действие **Отклонить**.

8. Если вы хотите чтобы по результатам проверки сообщения, содержащие вложенные объекты определенного размера, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок установлен.

9. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы для сообщений, содержащих вложенные объекты определенного размера, укажите текст меток в полях ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию метка не задана.

10. В поле **Размер сообщения (КБ)** введите максимальный размер объектов в диапазоне от 0 КБ до 1048576 КБ (1 ГБ).

    Если установлено значение 0 КБ, ограничения размера объектов отсутствуют.

    - по формату вложения;

11. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты определенного формата, в блоке параметров **Если обнаружен тип вложения** сформируйте список форматов вложений, к которым должно применяться правило. Для этого выполните следующие действия:

    a. Выберите способ формирования списка:

       - **Вложения, тип которых указан в списке**, если вы хотите указать форматы вложений, которые требуется добавить в список.

         К сообщениям, содержащим вложения указанных форматов, будут применяться параметры контентной фильтрации.

       - **Вложения, тип которых НЕ указан в списке**, если вы хотите указать форматы вложений, которые требуется исключить из списка.

         К сообщениям, содержащим вложения указанных форматов, не будут применяться параметры контентной фильтрации.

    b. По ссылке **Заменить** откройте окно **Формат файла**.

    c. Установите флажки рядом с форматами вложений, которые вы хотите добавить в список или исключить из списка:

       - архивы (например, ZIP; RAR; TGZ);
       - базы данных (например, ACCDB; ACCDC; MDB);
       - исполняемые файлы (например, EXE; DLL; OCX);
       - графические файлы (например, JPG; BMP; WMF);
       - файлы мультимедиа (например, AVI; WMV; MP3);
       - файлы документов (например, DOC; XLS; PDF; PPT);
       - прочие файлы (например, TXT; CHM; HTM).

    d. В правом нижнем углу нажмите на кнопку ОК.

12. В раскрывающемся списке **В случае обнаружения** выберите действие, которое будет применяться к сообщениям:

- **Пропустить**.
- **Удалить сообщение**.
- **Удалить вложение**.
- **Отклонить**.

По умолчанию выбрано действие **Отклонить**.

13. Если вы хотите чтобы по результатам проверки сообщения, содержащие вложения указанных форматов, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок установлен.

14. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы для сообщений, содержащих вложенные объекты определенного формата, укажите текст меток в полях ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию метка не задана.

    - по маске имени вложения.

15. Если вы хотите ограничить пересылку сообщений, содержащих вложенные объекты с определенными именами, в блоке параметров **Имя вложения** в поле **Имена вложений** введите маски имен вложенных объектов, пересылку сообщений с которыми вы хотите ограничить.

    Маски могут содержать любые символы. Разделяйте маски знаком ";".

    Например, вы можете ввести маску имени `*.exe` и ограничить пересылку сообщений, содержащих вложенные объекты с расширением exe.

16. В раскрывающемся списке **В случае обнаружения** выберите действие, которое будет применяться к сообщениям:

    - **Пропустить**.
    - **Удалить сообщение**.
    - **Удалить вложение**.
    - **Отклонить**.

    По умолчанию выбрано действие **Отклонить**.

17. Если вы хотите чтобы по результатам проверки сообщения, содержащие вложения с указанными именами, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

    По умолчанию флажок установлен.

18. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы для сообщений, содержащих вложенные объекты определенного формата, укажите текст меток в полях ввода под флажком **Поместить копию в Хранилище**.

    По умолчанию метка не задана.

19. Если вы хотите проверять наличие запрещенных форматов или имен файлов внутри составных объектов (в том числе внутри архивов), установите флажок **Проверять составные объекты**.

Если вы включите проверку составных объектов, флажок **Проверять форматы и имена файлов внутри архивов** будет установлен автоматически, так как архивы являются разновидностью составных объектов.

20. Если на предыдущем шаге вы не включили проверку составных объектов и хотите проверять наличие запрещенных форматов или имен файлов только внутри архивов, установите флажок **Проверять форматы и имена файлов внутри архивов**.
21. Нажмите на кнопку **Сохранить**.

Контентная фильтрация будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что контентная фильтрация сообщений для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Проверка подлинности отправителей сообщений

Перед тем как настроить параметры проверки подлинности в правиле обработки сообщений, убедитесь, что соответствующая проверка подлинности отправителей включена в общих параметрах защиты.

► *Чтобы настроить проверку подлинности отправителей сообщений в правиле обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить проверку подлинности отправителей сообщений.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Проверка подлинности**.
5. Включите или отключите проверку подлинности отправителей сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию проверка подлинности отключена.
6. Если на предыдущем шаге вы включили проверку подлинности, настройте общие параметры для всех типов проверок:
   - Установите флажок **Считать временные ошибки (TempError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Secure Mail Gateway считал временные ошибки TempError нарушением подлинности отправителя сообщений.

- Установите флажок **Считать постоянные ошибки (PermError) нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Secure Mail Gateway считал постоянные ошибки PermError нарушением подлинности отправителя сообщений.

7. Настройте параметры проверок следующих типов:

   - DMARC-проверка.

Перед тем как настроить параметры DMARC-проверки сообщений для правила, убедитесь, что DMARC-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

1. В блоке параметров **DMARC-проверка подлинности отправителей** установите флажок **Считать результат DMARC-проверки приоритетным**, если вы хотите, чтобы Kaspersky Secure Mail Gateway определял нарушение подлинности отправителя сообщений только по результатам DMARC-проверки, не учитывая результаты SPF- и DKIM-проверок.

   Если флажок установлен, нарушение подлинности отправителя сообщений определяется по результатам DMARC-проверки. Если флажок снят, результаты SPF-, DKIM- и DMARC-проверок считаются равнозначными. Нарушение при любой из этих проверок считается нарушением подлинности отправителя. При нарушении по нескольким проверкам одновременно, над сообщением выполняется самое строгое из заданных действий над сообщением при SPF-, DKIM- или DMARC-нарушениях подлинности отправителя.

2. В раскрывающемся списке **Если обнаружено DMARC-нарушение** выберите одно из следующих действий над сообщениями, DMARC-проверка которых выявила нарушение подлинности отправителя сообщений:

   - **Применить DMARC-политику**.

     DMARC-политика задается администратором на DNS-сервере. Если администратор установил политику None или Quarantine, программа выполнит действие **Пропустить**. Политике Reject соответствует действие программы **Отклонить**.

   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

   По умолчанию выбрано действие **Применить DMARC-политику**.

3. Если вы хотите чтобы сообщения, DMARC-проверка которых выявила нарушение подлинности, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок снят.

4. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, DMARC-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию метка не задана.

- SPF-проверка.

Перед тем как настроить параметры SPF-проверки сообщений для правила, убедитесь, что SPF-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

1. В блоке параметров **SPF-проверка подлинности отправителей** установите флажок **Считать SPF softfail нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Secure Mail Gateway считал ошибку SPF softfail, обнаруженную при SPF-проверке, нарушением подлинности отправителя сообщений.
2. В раскрывающемся списке **Если обнаружено SPF-нарушение** выберите одно из следующих действий над сообщениями, SPF-проверка которых выявила нарушение подлинности отправителя сообщений:
   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

   По умолчанию выбрано действие **Пропустить**.
3. Если вы хотите чтобы сообщения, SPF-проверка которых выявила нарушение подлинности, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок снят.
4. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, SPF-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию метка не задана.

- DKIM-проверка.

Перед тем как настроить параметры DKIM-проверки сообщений для правила, убедитесь, что DKIM-проверка подлинности отправителей сообщений включена в общих параметрах защиты.

1. В блоке параметров **DKIM-проверка подлинности отправителей** установите флажок **Считать отсутствие DKIM-подписи нарушением подлинности отправителя**, если вы хотите, чтобы Kaspersky Secure Mail Gateway считал отсутствие DKIM-подписи к сообщению, обнаруженное при DKIM-проверке, нарушением подлинности отправителя сообщения.
2. В раскрывающемся списке **Режим сопоставления** выберите режим аутентификации:
   - **Расслабленный**.
   - **Строгий**.
3. В раскрывающемся списке **Если обнаружено DKIM-нарушение** выберите одно из следующих действий над сообщениями, DKIM-проверка которых выявила нарушение подлинности отправителя сообщений:
   - **Отклонить**.
   - **Удалить сообщение**.
   - **Пропустить**.

   По умолчанию выбрано действие **Пропустить**.

4. Если вы хотите чтобы сообщения, DKIM-проверка которых выявила нарушение подлинности, автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок снят.

5. Если вы хотите, чтобы по результатам проверки программа добавляла метки в начало темы сообщений, DKIM-проверка которых выявила нарушение подлинности, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию метка не задана.

8. Нажмите на кнопку **Сохранить**.

Проверка подлинности отправителей сообщений будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что проверка подлинности для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Настройка уведомлений о событиях проверки сообщений

Вы можете настроить отправку почтовых уведомлений о событиях проверки сообщений для одного или нескольких правил.

Доступно, если отправка уведомлений включена в общих параметрах (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 264) почтовых уведомлений.

Вы можете настроить отправку почтовых уведомлений адресатам из общего списка, отправителю, получателю сообщений или другим адресатам о следующих событиях проверки сообщений:

- **Обнаружены вредоносные объекты**.
- **Обнаружены зашифрованные объекты**.
- **Обнаружены ошибки проверки модулем Антивирус**.
- **Обнаружены проблемы с контентной фильтрацией**.
- **Обнаружены сообщения, содержащие фишинг**.
- **Обнаружен макрос во вложении**.
- **Обнаружены вредоносные ссылки**.
- **Если KATA сервер обнаружил объект**.

► Чтобы настроить отправку уведомлений о событиях проверки сообщений, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Правила**.

2. В таблице правил выберите правило, для которого вы хотите настроить уведомления о событиях проверки.

   Откроется окно **Просмотреть правило**.

3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Уведомления**.

5. В блоке параметров с названием выбранного события (например, **Обнаружены вредоносные объекты**) установите флажки рядом с названиями параметров:

   - **Уведомить получателей из общего списка**, если вы хотите включить отправку уведомлений о выбранном событии на адреса из общего списка.

     Если флажок установлен, вам требуется задать список адресов, перейдя по ссылке **Настроить** в общие параметры почтовых уведомлений (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 264).

   - **Уведомить отправителя**, если вы хотите включить отправку уведомлений о выбранном событии на адреса отправителей сообщений.
   - **Уведомить получателя**, если вы хотите включить отправку уведомлений о выбранном событии на адреса получателей сообщений.
   - **Дополнительные адреса**, если вы хотите включить отправку уведомлений о выбранном событии на дополнительные адреса электронной почты.

6. Если вы включили отправку уведомлений на адреса получателей сообщений, выберите один из следующих вариантов:

   - **Только уведомлять**, если вы хотите настроить отправку уведомления без оригинала сообщения.
   - **Уведомлять с оригиналом сообщения во вложении**, если вы хотите настроить отправку уведомления с оригиналом сообщения во вложении.

7. Если вы включили отправку уведомлений на дополнительные адреса электронной почты, укажите адрес в поле ввода и нажмите на клавишу **ENTER**.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "re:".

   Регулярные выражения нечувствительны к регистру.

8. Если требуется, по ссылке **Настроить шаблоны уведомлений** в правом верхнем углу окна измените шаблоны уведомлений (см. раздел "Настройка шаблонов уведомлений" на стр. 265).

9. Нажмите на кнопку **Сохранить**.

Уведомления о событиях проверки сообщений будут настроены.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Добавление предупреждения о небезопасном сообщении

► Чтобы добавить предупреждение о небезопасном сообщении, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить предупреждение о небезопасном сообщении.

   Откроется окно **Просмотреть правило**.
3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.
4. В левой панели выберите раздел **Предупреждение о небезопасном сообщении**.
5. В раскрывающемся списке **Шаблон предупреждения** выберите шаблон предупреждения о небезопасном сообщении, которое вы хотите добавить.
6. Установите флажки рядом с одним или несколькими из следующих типов сообщений, к которым вы хотите добавить предупреждение:
   - **Для зашифрованных сообщений**.
   - **Для фишинговых сообщений**.
   - **Для зараженных сообщений**.
   - **Для сообщений с ошибками проверки модулем Антивирус**.
   - **Для сообщений, содержащих ссылки**.
7. Нажмите на кнопку **Сохранить**.

Предупреждения будут добавляться в текст сообщений согласно заданным параметрам.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Добавление примечания к событиям проверки сообщений

► *Чтобы добавить примечание к событию проверки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.

2. В таблице правил выберите правило, для которого вы хотите настроить примечание к событию проверки сообщений.

   Откроется окно **Просмотреть правило**.

3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Примечание к сообщению**.

5. Включите или отключите добавление примечания к событию проверки сообщений с помощью переключателя справа от названия раздела.

   По умолчанию добавление примечания отключено.

6. В раскрывающемся списке **Добавить примечание** выберите шаблон примечания, которое вы хотите добавить к событию проверки сообщений.

7. Нажмите на кнопку **Сохранить**.

Добавление примечания к событиям проверки сообщений будет настроено.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что добавление примечаний к сообщениям для правила включено, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Настройка защиты KATA

Перед тем как настроить параметры защиты KATA в правиле обработки сообщений, убедитесь, что интеграция с KATA настроена (см. раздел "Защита KATA" на стр. 228) в общих параметрах защиты.

► *Чтобы настроить защиту KATA в правиле обработки сообщений:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить защиту KATA.

   Откроется окно **Просмотреть правило**.

3. Нажмите на кнопку **Изменить**.

   Параметры правила станут доступны для редактирования.

4. В левой панели выберите раздел **Защита KATA**.
5. Включите или отключите защиту KATA для сообщений, попадающих под критерии правила, с помощью переключателя справа от названия раздела.

   По умолчанию защита KATA отключена.

6. Если на предыдущем шаге вы включили защиту KATA, в раскрывающемся списке **В случае обнаружения** выберите действие, которое будет применяться к сообщениям:

   - **Удалить сообщение**.

- **Отклонить**.
- **Пропустить**.

По умолчанию выбрано действие **Удалить сообщение**.

7. Если вы хотите чтобы по результатам проверки на сервере KATA сообщения с обнаруженными объектами автоматически помещались в Хранилище, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок установлен.

8. Если вы хотите, чтобы по результатам проверки программа добавляла метку в начало темы для сообщений, в которых обнаружены объекты по результатам проверки KATA, укажите текст метки в поле ввода под флажком **Поместить копию в Хранилище**.

   По умолчанию добавлена метка *[KATA detect]*.

9. Нажмите на кнопку **Сохранить**.

Защита KATA будет настроена. К сообщениям, попадающим под критерии правила, будут применяться заданные параметры.

Для того чтобы настроенные вами параметры использовались в работе Kaspersky Secure Mail Gateway, убедитесь, что защита KATA для правила включена, и что правило, для которого вы настроили параметры, включено (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

Просмотр информации о правиле

► *Чтобы просмотреть информацию о правиле, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Выберите правило, информацию о котором вы хотите просмотреть.

   Откроется окно **Просмотреть правило**.

Окно содержит следующие разделы:

- **Общие**.
- **Антивирус**.
- **Проверка ссылок**.
- **Анти-Спам**.
- **Анти-Фишинг**.
- **Контентная фильтрация**.
- **Проверка подлинности**.
- **Уведомления**.
- **Предупреждение о небезопасном сообщении**.
- **Примечание к сообщению**.

- **Защита KATA**.

  Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

Включение и отключение правила обработки сообщений

► *Чтобы включить или отключить правило обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Выполните одно из следующих действий:
   - Включите переключатель в строке с названием того правила, которое вы хотите включить.
   - Выключите переключатель в строке с названием того правила, которое вы хотите отключить.

Изменение параметров правила

► *Чтобы изменить параметры правила, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Выберите правило, параметры которого вы хотите изменить.

   Откроется окно **Просмотреть правило**.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить правило**.
4. Внесите необходимые изменения.
5. Нажмите на кнопку **Сохранить**.

Параметры правила будут изменены.

Удаление правил обработки сообщений

► *Чтобы удалить правило обработки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Выберите правило, которое вы хотите удалить.

   Откроется окно **Просмотреть правило**.
3. В правом нижнем углу нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **ОК**.

Правило обработки сообщений будет удалено.

kaspersky

Списки разрешенных и запрещенных адресов

Списки разрешенных и запрещенных адресов предоставляют возможность более точно настроить реакцию почтовой системы на сообщения с определенных адресов. Например, вы можете добавить в список разрешенных адреса источников, не являющиеся спамом официально, но определяемые программой как массовые рассылки (к примеру, сообщения с новостных порталов).

Вы можете настроить списки разрешенных и запрещенных адресов следующими способами:

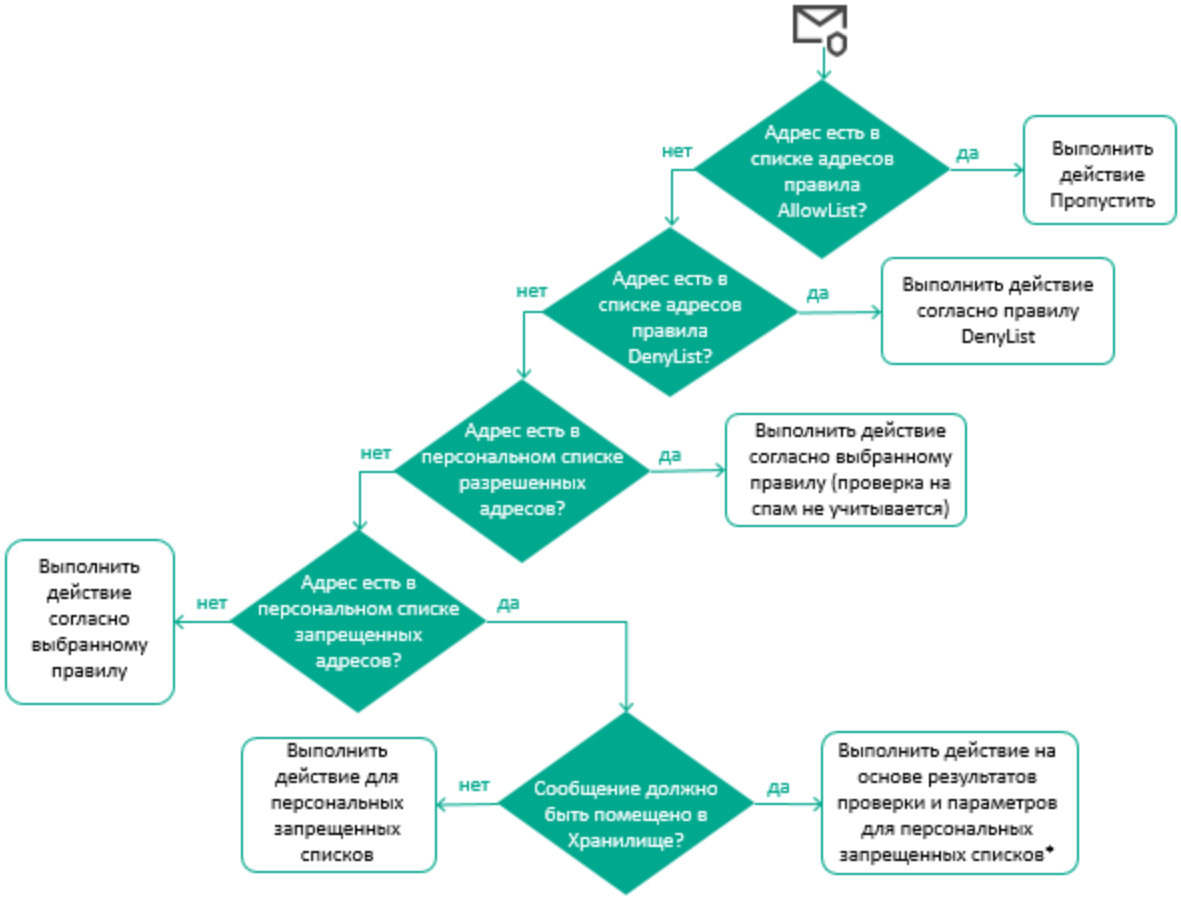
- С помощью предустановленных правил обработки сообщений AllowList и DenyList. Вы также можете создать свои правила с указанием адресов отправителей и получателей, к сообщениям от которых нужно применять заданное действие, и изменить их приоритет.

  По умолчанию правила AllowList и DenyList отключены, и в них не указаны адреса отправителей и получателей. Вам требуется сформировать в этих правилах списки адресов (см. раздел "Изменение параметров правила" на стр. 122) и включить их использование (см. раздел "Включение и отключение правила обработки сообщений" на стр. 122).

- С помощью персональных списков разрешенных и запрещенных адресов, которые содержат адреса отправителей сообщений для одного получателя. Персональный список разрешенных адресов пропускает сообщения без проверки на спам. При этом выполняется проверка на фишинг, вирусы и другие программы, представляющие угрозу, а также выполняется контентная фильтрация.

Алгоритм обработки сообщений согласно спискам разрешенных и запрещенных адресов, установленный по умолчанию, схематически представлен на рисунке ниже. Вы можете изменять действие для правила DenyList (**Отклонить** или **Удалить сообщение**), а также изменять приоритет правил, перемещая правила

AllowList и DenyList в таблице правил. В этом случае алгоритм применения действий программы будет отличаться от описанного ниже.



Обработка сообщения, адреса отправителя и получателей которого состоят в списке разрешенных или запрещенных адресов в правилах обработки сообщений, выполняется следующим образом:

- Если адреса отправителя и получателей сообщения состоят в списке разрешенных адресов в правиле AllowList, по умолчанию программа пропускает сообщение без проверки.
- Если адреса не указаны в правиле AllowList, выполняется проверка по списку запрещенных адресов в правиле DenyList. Если адреса отправителя и получателей найдены в списке, по умолчанию программа отклоняет сообщение, не выполняя проверку. Вы можете изменить действие правила DenyList.

Если сообщение не попадает под действие списков разрешенных и запрещенных адресов в правилах обработки сообщений, то программа проверяет, находится ли адрес отправителя сообщения в персональных списках получателя:

- Если адрес отправителя содержится в персональном списке разрешенных адресов, то проверка модулем Анти-Спам не выполняется. Сообщение обрабатывается согласно результатам проверки других модулей программы.
- Если адрес отправителя сообщения не состоит в персональном списке разрешенных адресов получателя этого сообщения, то выполняется проверка по персональному запрещенному списку. В случае совпадения сообщение не доставляется получателю – владельцу персонального списка запрещенных адресов. В зависимости от указанного действия (см. раздел "Настройка параметров

персональных списков" на стр. 125) программа удаляет или отклоняет сообщение. Также программа может поместить сообщение в Хранилище.

> * Перед тем, как поместить копию сообщения в Хранилище, программа проверяет его с помощью всех модулей защиты. По результатам проверки программа выполняет над сообщением наиболее строгое действие. Например, если в результате проверки должно быть применено правило, в котором задано действие **Удалить сообщение**, а для персональных запрещенных списков задано действие **Отклонить**, то будет выполнено действие **Удалить сообщение** как более строгое, т.е. сообщение будет удалено согласно параметрам правила, а не отклонено согласно параметрам для персональных запрещенных списков.
> Сообщения, помещенные в Хранилище, не учитываются при подсчете сообщений со статусом *Персональный список запрещенных адресов* на графиках в разделе **Мониторинг**.

Если адреса не указаны ни в одном из списков ни в правилах обработки сообщений, ни в персональных списках получателя, то сообщение обрабатывается согласно выбранному правилу. Алгоритм выбора правила более подробно описан в главе про работу правил обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 98).

В этом разделе

Настройка параметров персональных списков

> Параметры этого раздела применяются ко всем персональным учетным записям.

► *Чтобы настроить параметры персональных списков разрешенных и запрещенных адресов:*

1. В окне веб-интерфейса программы выберите раздел **Параметры → Персональные учетные записи → Списки запрещенных и разрешенных адресов**.
2. Включите или отключите отображение и использование списков разрешенных и/или запрещенных адресов с помощью переключателей **Список разрешенных адресов** и **Список запрещенных адресов**.

   > При включении персонального списка разрешенных или запрещенных адресов он становится доступным для просмотра и используется при обработке почтового трафика.

3. В раскрывающемся списке **Если адрес отправителя в списке запрещенных** выберите одно из следующих действий над сообщениями:
   - **Удалить сообщение**, если вы хотите удалять сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов.
   - **Отклонить**, если вы хотите отклонять сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов.

4. Если вы хотите помещать в Хранилище сообщения, адрес отправителя которых находится в персональном списке запрещенных адресов, установите флажок **Поместить копию в Хранилище**.

   По умолчанию флажок установлен.

5. Нажмите на кнопку **Сохранить**.

Параметры персональных списков разрешенных и запрещенных адресов будут настроены.

Просмотр персональных списков разрешенных и запрещенных адресов

Для работы с персональными списками разрешенных и запрещенных адресов из веб-интерфейса программы необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 225).

В режиме администратора вы можете просмотреть персональные списки разрешенных и запрещенных адресов всех пользователей, данные об учетных записях которых сохранены в LDAP-кеше.

В режиме пользователя отображаются только персональные списки текущего пользователя, если администратор включил отображение и использование персональных списков (см. раздел "Настройка параметров персональных списков" на стр. 125) в параметрах программы.

► *Чтобы просмотреть персональные списки разрешенных и запрещенных адресов в режиме администратора:*

1. Подключитесь к веб-интерфейсу программы, используя учетные данные администратора программы.
2. В окне веб-интерфейса программы выберите раздел **Пользовательские списки**.
3. В поле ввода укажите имя пользователя в формате distinguishedName в службе каталогов LDAP.

   Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.

4. Нажмите на LDAP-запись пользователя, списки которого вы хотите просмотреть.
5. Нажмите на кнопку **Найти** справа от поля ввода.

В рабочей области отобразятся списки разрешенных и запрещенных адресов выбранного пользователя.

► *Чтобы просмотреть персональные списки разрешенных и запрещенных адресов в режиме пользователя:*

1. Подключитесь к веб-интерфейсу программы, используя доменные учетные данные пользователя.
2. Выберите раздел **Пользовательские списки**.

В рабочей области отобразятся списки разрешенных и запрещенных адресов текущего пользователя.

kaspersky

Формирование персональных списков

Для получения доступа к персональным спискам разрешенных и запрещенных адресов из веб-интерфейса программы необходимо добавить соединение с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 225).

В режиме администратора вы можете добавлять, изменять и удалять адреса в персональных списках всех пользователей, данные об учетных записях которых сохранены в LDAP-кеше.

В режиме пользователя вы можете просматривать и изменять персональные списки только текущего пользователя.

► *Чтобы сформировать персональные списки разрешенных и запрещенных адресов:*

1. Если вы находитесь в режиме администратора, выполните следующие действия:
   a. В окне веб-интерфейса программы выберите раздел **Пользовательские списки**.
   b. В поле ввода укажите имя пользователя в формате distinguishedName в службе каталогов LDAP.

      Под полем ввода отобразится список LDAP-записей, содержащих совпадения с указанной вами строкой поиска.
   c. Нажмите на LDAP-запись пользователя, списки которого вы хотите изменить.
   d. Нажмите на кнопку **Найти** справа от поля ввода.
2. Если вы находитесь в режиме пользователя, выберите раздел **Пользовательские списки**.

   В рабочей области отобразятся персональные списки – в левой части список разрешенных адресов, в правой части список запрещенных адресов.

   Выполните шаги 3-5 для каждого персонального списка.
3. Если вы хотите добавить в персональный список новый адрес, укажите его в поле ввода и нажмите клавишу **ENTER**.

   Вы можете добавлять адреса по одному или ввести несколько адресов, разделенных точкой с запятой.

   Вы можете использовать символы "*" и "?" для создания масок адресов. Поддерживается добавление интернационализированных адресов.
4. Если вы хотите изменить ранее добавленный адрес, нажмите на него в поле ввода, внесите необходимые изменения в режиме редактирования и нажмите клавишу **ENTER**.
5. Если вы хотите удалить адрес из персонального списка, нажмите на значок ✕ справа от адреса.
6. Нажмите на кнопку **Сохранить**.

   Если хотя бы один из адресов указан в недопустимом формате, сохранение списков недоступно. Исправьте все адреса, выделенные красным фоном, и повторите операцию сохранения еще раз.

Персональные списки разрешенных и запрещенных адресов будут сформированы.

kaspersky

Управление кластером

После установки и первоначальной настройки вы можете настраивать параметры в веб-интерфейсе программы. Для этого требуется объединить все узлы с установленной программой Kaspersky Secure Mail Gateway в кластер. Вы можете добавлять узлы в кластер (см. раздел "Добавление узла в кластер" на стр. 132) и удалять узлы из кластера (см. раздел "Удаление узла из кластера" на стр. 133). Вы можете назначить роль Управляющего узла любому из узлов, входящих в кластер. Остальные серверы в кластере получат роль Подчиненный узел. Независимо от роли все узлы кластера будут осуществлять обработку трафика.

Все узлы должны быть добавлены в кластер по IP-адресу одинакового формата (только IPv4 или только IPv6).

Таблица узлов кластера отображается в веб-интерфейсе программы в разделе **Узлы**.

В этом разделе

Создание нового кластера

После установки программы требуется создать кластер для управления узлами через веб-интерфейс программы. Кроме того, вы можете создать несколько кластеров, чтобы управлять разными группами серверов отдельно друг от друга.

► *Чтобы создать новый кластер, выполните следующие действия:*

1. В веб-интерфейсе узла, которому вы хотите назначить роль Управляющий узел, нажмите на кнопку **Создать новый кластер**.
2. Через несколько минут обновите страницу браузера.

   Откроется веб-интерфейс Управляющего узла.

Кластер будет создан. После этого вы можете добавлять в кластер Подчиненные узлы (см. раздел "Добавление узла в кластер" на стр. 132).

kaspersky

Просмотр таблицы узлов кластера

► *Чтобы просмотреть таблицу узлов кластера,*

в окне веб-интерфейса программы выберите раздел **Узлы**.

В таблице отображается следующая информация об узлах кластера:

- **IP-адрес:порт** – IP-адрес и порт подключения узла кластера.
- **Роль** – роль узла в кластере.
- **Статус** – информация о наличии проблем на узле.

  При отображении статуса учитывается следующая информация об узле:

  - состояние подключения к серверам KSN/KPSN;
  - статус лицензионного ключа;
  - актуальность баз программы;
  - дата и время, а также результат выполнения последней задачи обновления;
  - состояние синхронизации времени с Управляющим узлом (для Подчиненных узлов).

  Возможны следующие статусы:

  - *Синхронизирован* – на узле нет проблем ни с одним из перечисленных параметров.
  - *Узел недоступен* – нет соединения с узлом (также указывается время, с которого узел стал недоступен).
  - При наличии ошибок по какому-либо параметру в графе перечисляются все ошибки (например, *Базы устарели, Уровень защиты снижен, Действие лицензии временно приостановлено*).
- **Комментарий** – любая дополнительная информация об узле.

При необходимости вы можете просмотреть детальную информацию (см. раздел "Просмотр информации об узле кластера" на стр. 130) о каждом узле кластера.

Настройка отображения таблицы узлов кластера

► *Чтобы настроить отображение таблицы узлов кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.

   Откроется таблица узлов кластера.
2. По кнопке **Настроить таблицу** откройте меню отображения таблицы узлов кластера.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   Должен быть установлен хотя бы один флажок.

Отображение таблицы узлов кластера будет настроено.

Просмотр информации об узле кластера

► *Чтобы просмотреть информацию об узле кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. Выберите узел, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об узле.

Окно содержит следующую информацию в зависимости от типа сервера:

1. Блок параметров **Информация об узле**:
   - **Отпечаток сертификата:** – отпечаток сертификата сервера.
   - **Технология виртуализации** – название платформы виртуализации.

     Возможны следующие значения:
     - **ACRN**.
     - **bhyve (гипервизор FreeBSD™)**.
     - **Bochs Emulator**.
     - **Linux KVM**.
     - **Microsoft Hyper-V**.
     - **Не используется** – программа установлена на физическом сервере.
     - **Oracle® VM VirtualBox**.
     - **Parallels Desktop® или Server**.
     - **QEMU**.
     - **QNX**.
     - **UML (user-mode Linux)**.
     - **VMware™ Workstation или Server**.
     - **Xen**.
     - **z/VM**.

     > В программе Kaspersky Secure Mail Gateway поддерживаются гипервизоры Microsoft Hyper-V и VMware ESXi. Работоспособность программы при использовании других гипервизоров не гарантируется.

   - **Комментарий** – дополнительная информация об узле. Необязательный параметр.
   - **Роль текущего сервера** – роль текущего узла в кластере.
   - **Количество потоков проверки** – количество одновременных потоков обработки трафика ICAP-сервером.

2. Блок параметров **Параметры**:
   - Для Управляющего узла:
     - **Применены** – время последнего успешного применения параметров к модулям программы.
     - **Время** – состояние синхронизации времени с гипервизором и с NTP-сервером.
   - Для Подчиненного узла:
     - **Синхронизирован** – время последнего успешного получения параметров от Управляющего узла. Если параметры получены, вы можете назначить этому Подчиненному узлу роль Управляющего без потери заданных параметров.
     - **Применены** – время последнего успешного применения параметров к модулям программы.
3. Блок параметров **Информация о базах**:
   - **Обновление баз** – состояние баз программы, а также результат и время их последнего успешного обновления.
   - **Антивирус** – состояние баз модуля Антивирус.
   - **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.
   - **Анти-Спам** – состояние баз модуля Анти-Спам.

   Возможны следующие значения:
   - *Базы обновлены*.
   - *Базы устарели*.
   - *Базы сильно устарели*.
   - *Ошибка баз*.
4. Блок параметров **Внешние службы**:
   - **Состояние соединения с KSN/KPSN** – состояние соединения со службами KSN / KPSN.
   - **KATA статус** – состояние подключения к серверу KATA (отображается только при настроенной интеграции с KATA).
   - **Состояние keytab-файла Kerberos** – наличие SPN-записей обо всех Подчиненных узлах в keytab-файле (отображается только при включенной Kerberos-аутентификации).
   - Блок параметров **Состояние LDAP** (отображается только при настроенной интеграции с доменом Active Directory):
     - **Подключение** – дата и время последнего успешного подключения к контроллеру домена Active Directory.
     - **Данные для подбора правил** – дата и время последнего успешного обновления данных об учетных записях, используемых для подбора правил обработки трафика.
     - **Автозаполнение учетных записей** – дата и время последнего успешного обновления данных, используемых для автозаполнения имен пользователей в веб-интерфейсе программы.

     Если хотя бы на одном из этих этапов возникла ошибка, в таблице узлов кластера отображается сообщение об ошибке.
5. Блок параметров **Дата и время** (отображается только для Подчиненных узлов):
   - **Время** – состояние синхронизации времени:

- с сервером, на котором установлен Управляющий узел;
- с гипервизором;
- с NTP-сервером.

Если статус имеет значение *Ошибка*, вы можете скопировать информацию об ошибке в буфер обмена по кнопке справа от статуса.

6. Блок параметров **Информация о лицензии**:
   - **Дата окончания срока действия лицензии**.
   - **Лицензия** – информация о состоянии лицензионного ключа (для активного лицензионного ключа указывается также дата окончания срока действия и количество дней до его истечения).
   - **Программа** – название программы, для которой предназначен добавленный лицензионный ключ.
   - **Уровень функциональности** – режим работы программы (см. раздел "Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией" на стр. 41) в зависимости от добавленного лицензионного ключа.
   - **Тип лицензии** – тип лицензии (пробная, коммерческая или подписочная).
   - **Серийный номер** – серийный номер лицензионного ключа.

Добавление узла в кластер

► *Чтобы добавить узел в кластер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. Нажмите на кнопку **Добавить узел**.

   Откроется окно **Добавить узел**.
3. В поля **IP-адрес** и **Порт** введите IP-адрес и порт сервера с установленной программой, который вы хотите добавить в качестве узла кластера.
4. Если требуется, в поле **Комментарий** укажите дополнительную информацию о добавляемом узле.
5. В поле **Количество потоков проверки** укажите, сколько потоков трафика может обрабатывать почтовый сервер одновременно.

   Значение по умолчанию – 16.
6. Нажмите на кнопку **Далее**.
7. Сравните отпечаток сертификата в окне **Проверка узла** с отпечатком сертификата сервера. Если отпечатки сертификата совпадают, нажмите на кнопку **Подтвердить**.

   Отпечаток сертификата отображается в локальной консоли сервера после завершения мастера первоначальной настройки.

Узел будет добавлен в кластер и отобразится в таблице узлов на странице **Узлы**.

Прежде чем направить на добавленный узел почтовый трафик, требуется обновить базы программы (см. раздел "Запуск обновления баз вручную" на стр. 218) и выполнить LDAP-синхронизацию (см. раздел "Запуск синхронизации с контроллером домена Active Directory вручную" на стр. 227). В противном случае программа не сможет обеспечить должный уровень защиты, не сможет помещать сообщения электронной почты в Персональное Хранилище, а правила, в которых указаны атрибуты учетных записей Active Directory, не будут применены.

Изменение параметров узла

Вы не можете изменить IP-адрес и порт сервера, на котором установлена программа. При необходимости удалите узел из кластера (см. раздел "Удаление узла из кластера" на стр. 133) и добавьте в кластер новый узел (см. раздел "Добавление узла в кластер" на стр. 132) с нужным адресом.

► *Чтобы изменить параметры узла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите узел, параметры которого вы хотите изменить.

   Откроется окно параметров узла.
3. В правом нижнем углу окна нажмите на кнопку **Изменить**.

   Откроется окно **Изменить узел**.
4. Если требуется, измените следующие параметры:
   - Дополнительную информацию об узле в поле **Комментарий**.
   - Количество одновременных потоков обработки трафика ICAP-сервером в поле **Количество потоков проверки**.

     Рекомендуемое значение: количество ядер процессора, умноженное на два.
5. Нажмите на кнопку **Сохранить**.

   Если вы изменили параметр **Количество потоков проверки**, сервер будет перезагружен. До завершения перезагрузки обработка трафика будет приостановлена.

Параметры узла будут изменены.

Удаление узла из кластера

Удаление Управляющего узла недоступно.

При удалении узла из кластера программа не удаляется с сервера. Вы можете в любой момент добавить узел обратно в кластер и продолжить управление параметрами программы для этого узла.

► *Чтобы удалить узел из кластера, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите удалить из кластера.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **ОК**.

Узел будет удален из кластера. Информация об узле не будет отображаться в таблице узлов кластера. Объекты, помещенные на карантин, резервные копии объектов, обновления баз, журналы событий, отчеты, а также полученная диагностическая информация сохраняются на сервере с установленной программой.

Изменение роли узла в кластере

Вы можете назначить любому узлу кластера роль Управляющий узел. Остальные узлы будут иметь роль Подчиненный узел. Например, смена ролей может понадобиться при выходе из строя Управляющего узла или при необходимости удалить программу с этого сервера.

► *Чтобы назначить Управляющему узлу роль Подчиненный узел, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Изменить роль на Подчиненный узел**.

Управляющий узел станет Подчиненным узлом. Откроется веб-интерфейс Подчиненного узла.

► *Чтобы назначить Подчиненному узлу роль Управляющий узел, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел.

   Откроется окно параметров узла.
3. Нажмите на кнопку **Перейти к управлению узлом**.

   В новом окне браузера откроется страница авторизации.
4. Введите имя и пароль администратора программы.

   Откроется веб-интерфейс Подчиненного узла.

5. Нажмите на кнопку **Изменить роль на Управляющий узел**.
6. В окне подтверждения нажмите на кнопку **ОК**.

Подчиненный узел станет Управляющим узлом.

Удаление кластера

Удаление кластера возможно только при отсутствии Подчиненных узлов.

► *Чтобы удалить кластер, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно параметров узла.
3. В левом нижнем углу окна нажмите на кнопку **Удалить кластер**.

   Отобразится окно подтверждения удаления узла из кластера.
4. Нажмите на кнопку **ОК**.

Кластер будет удален. Отобразится веб-интерфейс сервера с установленной программой, не входящего в кластер.

Перезагрузка узла кластера

Перезагрузка через веб-интерфейс доступна только для ISO-образа программы. При установке программы из rpm- или deb-пакета перезагрузка выполняется средствами операционной системы.

Перезагрузка операционной системы узла может быть необходима для применения некоторых обновлений, например, обновления библиотеки OpenSSL. В этом случае в таблице узлов кластера отображается уведомление *Требуется перезагрузить операционную систему*.

► *Чтобы перезагрузить Управляющий узел через веб-интерфейс программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Управляющий узел.

   Откроется окно с информацией об узле.
3. Нажмите на кнопку **Перезагрузить**.
4. В окне подтверждения нажмите на кнопку **ОК**.

Перезагрузка операционной системы будет запущена. Это может занять некоторое время. Обновите страницу браузера через несколько минут. После завершения перезагрузки откроется страница подключения к веб-интерфейсу программы.

До завершения перезагрузки обработка трафика будет остановлена.

► *Чтобы перезагрузить Подчиненный узел через веб-интерфейс программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. В таблице узлов кластера выберите Подчиненный узел, который вы хотите перезагрузить.

   Откроется окно с информацией об узле.
3. По ссылке **Перейти к управлению узлом** перейдите к веб-интерфейсу Подчиненного узла.

   Страница подключения к веб-интерфейсу откроется в новой закладке браузера.
4. Введите учетные данные и подключитесь к Подчиненному узлу.
5. Нажмите на кнопку **Перезагрузить**.
6. В окне подтверждения нажмите на кнопку **ОК**.

Перезагрузка операционной системы будет запущена. Это может занять некоторое время. Обновите страницу браузера через несколько минут. После завершения перезагрузки откроется страница подключения к веб-интерфейсу Подчиненного узла.

До завершения перезагрузки обработка трафика будет остановлена.

Проверка целостности данных

Проверка целостности модулей программы запускается автоматически после старта программы на узле кластера. Это позволяет убедиться, что компоненты программы установлены корректно, не изменены и не повреждены. Результаты выполненных проверок можно просмотреть (см. раздел "Просмотр информации о задачах проверки целостности" на стр. 137) в сводной таблице по узлам кластера.

Вы можете в любой момент запустить проверку целостности данных (см. раздел "Запуск проверки целостности вручную" на стр. 137) вручную. Проверка запускается для каждого узла кластера отдельно. При этом проверяются хеши исполняемых файлов программы по алгоритму ГОСТ Р 34.11-2012.

Если в результате проверки не было выявлено нарушений целостности, в окне просмотра результатов отобразится сообщение об этом. Если нарушения целостности обнаружены, вы сможете скачать архив со списком найденных проблем (см. раздел "Скачивание архива с результатом проверки" на стр. 138).

Информация о выполнении проверки целостности записывается в журнал событий (см. раздел "Типы системных событий" на стр. 173) и в журнал Syslog.

kaspersky

В этом разделе

Просмотр информации о задачах проверки целостности

► *Чтобы просмотреть информацию о задачах проверки целостности:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.

Отобразится таблица с информацией о выполненных задачах проверки целостности на узлах кластера:

- **IP-адрес:порт** – IP-адрес и порт подключения к узлу, для которого была запущена проверка целостности.
- **Роль** – роль узла в кластере.
- **Статус последней задачи**. Возможны следующие значения:
  - Прочерк, если проверка целостности ни разу не была запущена.
  - **В обработке** (с указанием процента выполнения задачи).
  - **Выполняется отмена**.
  - **Выполняется удаление**.
  - **Завершено** (с указанием времени завершения задачи).
  - **Завершено с ошибкой** (с указанием времени завершения задачи и описания ошибки).
  - **Ожидает**.

Запуск проверки целостности вручную

► *Чтобы запустить проверку целостности вручную:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите запустить проверку целостности.

   Откроется окно **Просмотреть архивы**.
4. В правом нижнем углу нажмите на кнопку **Запустить**.

Проверка целостности будет запущена.

Статус выполнения задачи отобразится в окне **Просмотреть архивы**, а также в таблице узлов кластера на странице **Проверка целостности данных**. Если будут выявлены нарушения целостности модулей программы, вы сможете скачать архив со списком найденных проблем (см. раздел "Скачивание архива с результатом проверки" на стр. 138).

Скачивание архива с результатом проверки

Архив с результатом проверки доступен для скачивания, только если были обнаружены нарушения целостности модулей. Если нарушений не обнаружено, отображается только сообщение об успешной проверке.

► *Чтобы скачать архив с результатом проверки:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите скачать архив с результатом проверки.

   Откроется окно **Просмотреть архивы**.
4. В строке с нужным архивом нажмите на значок справа от названия архива.

Архив будет сохранен на вашем компьютере в папке загрузки браузера.

Удаление архива с результатом проверки

► *Чтобы удалить архив с результатом проверки:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Проверить целостность данных** в верхней части рабочей области откройте окно **Проверка целостности данных**.
3. В таблице в рабочей области выберите узел кластера, для которого вы хотите удалить архив с результатом проверки.

   Откроется окно **Просмотреть архивы**.
4. В строке с нужным архивом нажмите на значок справа от названия архива.

Архив будет удален из списка.

kaspersky

Работа с ролями и учетными записями пользователей

Вы можете создавать различные роли для учетных записей пользователей программы в зависимости от прав, которыми они должны обладать. Список ролей и учетных записей пользователей, обладающих этими ролями, отображается в разделе **Учетные записи** веб-интерфейса программы.

Для каждой роли вы можете задать набор прав, которыми будет обладать роль. Кроме того, в программе доступны роли по умолчанию, создаваемые во время установки программы:

- Superuser с полным набором прав.
- Viewer, обладающая правами только на просмотр информации в веб-интерфейсе программы.

Удаление и изменение роли по умолчанию недоступно.

В этом разделе

Добавление роли

► *Чтобы добавить роль, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.

   Откроется список ролей.

2. Нажмите на кнопку **Добавить**.

   Откроется окно добавления роли.

3. В поле **Название роли** введите имя роли.
4. В блоке параметров **Права** установите флажки рядом с теми правами, которыми должна обладать роль:

Функциональная область	Название права	Описание
Мониторинг и отчеты	Просматривать разделы Мониторинг и Отчеты	При назначении этого права пользователь сможет только просматривать разделы **Мониторинг** и **Отчеты**, но не изменять их параметры.
	Изменять параметры в разделах Мониторинг и Отчеты	Это право позволяет пользователю изменять параметры отчетов, а также просматривать информацию в разделах **Мониторинг** и **Отчеты**.
Параметры	Просматривать параметры	При назначении этого права пользователь сможет только просматривать параметры программы в разделе **Параметры**, но не может изменять их.
	Изменять параметры	Это право позволяет пользователю изменять параметры программы в разделе **Параметры**. При назначении этого права пользователь сможет также просматривать параметры программы.
	Управлять доступом SSH	Это право позволяет пользователю подключиться к любому узлу кластера по протоколу SSH (см. раздел "Подключение к узлам кластера по протоколу SSH" на стр. 276), чтобы работать с программой в режиме Technical Support Mode через командную строку. При назначении этого права пользователь сможет также просматривать параметры программы.

Функциональная область	Название права	Описание
Правила	Просматривать правила	Это право позволяет пользователю только просматривать таблицу правил обработки сообщений (см. раздел "Просмотр таблицы правил" на стр. 99). Пользователь не сможет добавлять или удалять правила, а также изменять их параметры.
	Создавать/изменять правила	Это право позволяет пользователю добавлять правила обработки сообщений (см. раздел "Создание правила обработки сообщений" на стр. 102), а также изменять их параметры (см. раздел "Изменение параметров правила" на стр. 122).
	Удалять правила	Это право позволяет пользователю удалять правила обработки сообщений (см. раздел "Удаление правил обработки сообщений" на стр. 122).
События	Просматривать события обработки почтового трафика	Это право позволяет пользователю просматривать информацию о событиях обработки трафика (см. раздел "Просмотр журнала событий" на стр. 163).
	Просматривать системные события	Это право позволяет пользователю просматривать информацию о системных событиях (см. раздел "Просмотр журнала событий" на стр. 163).

Функциональная область	Название права	Описание
Учетные записи	Просматривать роли	Это право позволяет пользователю только просматривать список ролей в разделе **Учетные записи** (см. раздел "**Работа с ролями и учетными записями пользователей**" на стр. 139). Пользователь не сможет добавлять или удалять роли, а также изменять их параметры.
	Создавать/изменять/назначать/отзывать роли	Это право позволяет пользователю добавлять роли и изменять их параметры (см. раздел "Изменение параметров роли" на стр. 147). При назначении этого права пользователь сможет также просматривать список ролей в разделе **Учетные записи**.
	Удалять роли	Это право позволяет пользователю удалять роли (см. раздел "Удаление роли" на стр. 148). При назначении этого права пользователь сможет также просматривать список ролей в разделе **Учетные записи**.

Функциональная область	Название права	Описание
Узлы	Просматривать информацию об узлах	Это право позволяет пользователю только просматривать информацию об узлах в разделе **Узлы** (см. раздел "**Управление кластером**" на стр. 128). Пользователь не сможет добавлять и удалять серверы, а также изменять их параметры и роли.
	Создавать/изменять/удалять узлы	Это право позволяет пользователю добавлять (см. раздел "Добавление узла в кластер" на стр. 132) и удалять (см. раздел "Удаление узла из кластера" на стр. 133) узлы кластеров, а также изменять параметры (см. раздел "Изменение параметров узла" на стр. 133) и роли узлов (см. раздел "Изменение роли узла в кластере" на стр. 134) в кластере. При назначении этого права пользователь сможет также просматривать информацию об узлах кластера.
	Получать диагностическую информацию	Это право позволяет пользователю получать диагностическую информацию (см. раздел "Получение информации для Службы технической поддержки" на стр. 328) об узлах кластера. При назначении этого права пользователь сможет также просматривать информацию об узлах кластера.
	Проверять целостность данных	Это право позволяет пользователю запускать проверку целостности (см. раздел "Проверка целостности данных" на стр. 136) на узлах кластера, а также просматривать результаты выполнения проверки. При назначении этого права пользователь сможет также просматривать информацию об узлах кластера.

Функциональная область	Название права	Описание
Очередь сообщений	Просматривать информацию о сообщениях	Это право позволяет пользователю только просматривать информацию об очереди сообщений и Анти-Спам карантине в разделе **Очередь сообщений**.
	Выполнять принудительную отправку сообщений	Это право позволяет пользователю принудительно отправить сообщение вне очереди (см. раздел "Принудительная отправка сообщений из очереди" на стр. 181). При назначении этого права пользователь сможет также просматривать информацию об очереди сообщений и Анти-Спам карантине.
	Удалять сообщения	Это право позволяет пользователю удалять сообщения из очереди (см. раздел "Принудительная отправка сообщений из очереди" на стр. 181). При назначении этого права пользователь сможет также просматривать информацию об очереди сообщений и Анти-Спам карантине.
Хранилище	Просматривать сообщения	Это право позволяет пользователю только просматривать информацию об объектах в Хранилище в разделе **Хранилище**.
	Доставлять сообщения	Это право позволяет пользователю доставлять получателям те сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища" на стр. 160), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.

Функциональная область	Название права	Описание
	Доставлять небезопасные сообщения	Это право позволяет пользователю доставлять получателям любые сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища" на стр. 160). При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.
	Пересылать сообщения на любые адреса	Это право позволяет пользователю пересылать на любые адреса те сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища" на стр. 160), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.
	Пересылать небезопасные сообщения на любые адреса	Это право позволяет пользователю пересылать на любые адреса любые сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища" на стр. 160). При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.
	Удалять сообщения	Это право позволяет пользователю удалять копии сообщений из хранилища (см. раздел "Удаление копии сообщения из Хранилища" на стр. 162). При назначении этого права пользователь сможет также просматривать информацию об объектах в хранилище.

Функциональная область	Название права	Описание
	Сохранять сообщения	Это право позволяет пользователю скачивать копии тех сообщений из Хранилища (см. раздел "Скачивание сообщения из Хранилища" на стр. 161), в которых модули Антивирус, Анти-Фишинг и Проверка ссылок не обнаружили угроз. При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.
	Сохранять небезопасные сообщения	Это право позволяет пользователю скачивать копии любых сообщений из Хранилища (см. раздел "Скачивание сообщения из Хранилища" на стр. 161). При назначении этого права пользователь сможет также просматривать информацию об объектах в Хранилище.
Списки запрещенных и разрешенных адресов	Просматривать все списки разрешенных и запрещенных адресов	Это право позволяет пользователю только просматривать персональные списки разрешенных и запрещенных адресов (см. раздел "Просмотр персональных списков разрешенных и запрещенных адресов" на стр. 126). Пользователь не сможет изменять состав этих списков.
	Управлять всеми списками разрешенных и запрещенных адресов	Это право позволяет пользователю добавлять, удалять и изменять адреса в персональных списках (см. раздел "Формирование персональных списков" на стр. 127) разрешенных и запрещенных адресов. При назначении этого права пользователь сможет также просматривать все персональные списки.

5. Нажмите на кнопку **Добавить**.

Роль будет добавлена.

Разделы веб-интерфейса программы будут отображаться в соответствии с правами роли, назначенной пользователю, после следующей аутентификации пользователя в веб-интерфейсе.

Просмотр информации о роли

► *Чтобы просмотреть информацию о роли, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.

   Откроется список ролей.

2. В левой части окна выберите роль, информацию о которой вы хотите просмотреть.

Отобразится следующая информация:

- На закладе **Пользователи** отображается список учетных записей пользователей, которым назначена выбранная роль. Вы можете отзывать роль (см. раздел "Отзыв роли" на стр. 148) или назначать ее новым пользователям (см. раздел "Назначение роли" на стр. 148).
- На закладке **Разрешения** отображается набор прав, которые получает пользователь при назначении ему этой роли. Вы можете изменять список прав для выбранной роли (см. раздел "Изменение параметров роли" на стр. 147).

Изменение параметров роли

Изменение роли Superuser недоступно.

Вы можете изменить параметры роли: название роли, а также набор прав, которыми она обладает.

► *Чтобы изменить параметры роли, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.

   Откроется список ролей.

2. Выберите роль, для которой хотите изменить параметры.
3. Нажмите на кнопку **Изменить роль** справа от поля Roles.
4. Также вы можете перейти на закладку **Разрешения** в правой части окна и нажать кнопку **Изменить**.

   Откроется окно **Изменить роль**.

5. Если требуется, измените название роли в поле **Название роли**.
6. Если требуется, измените набор прав, которыми обладает роль. Для этого снимите или установите флажки в блоке параметров **Разрешения**.
7. Нажмите на кнопку **Сохранить**.

Параметры роли будут изменены.

Удаление роли

► *Чтобы удалить роль, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.

   Откроется список ролей.
2. Выберите роль, которую вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

   Отобразится окно подтверждения удаления роли.
4. Нажмите на кнопку **Да**.

Роль будет удалена.

Назначение роли

► *Чтобы назначить роль пользователю, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.
2. Откроется список ролей.
3. Выберите роль, которую вы хотите назначить пользователю.
4. Перейдите на закладку **Пользователи** в правой части окна.
5. Нажмите на кнопку **Назначить роль**.

   Откроется окно **Назначить роль**.
6. Введите `домен\имя` (NTLM) или `user@REALM` (Kerberos) для пользователя, которому вы хотите назначить роль.
7. Нажмите на кнопку **Сохранить**.

Роль будет назначена выбранному пользователю.

Отзыв роли

► *Чтобы отозвать роль у пользователя, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **Учетные записи**.

   Откроется список ролей.
2. Выберите роль, которую вы хотите отозвать.

3. Перейдите на закладку **Пользователи** в правой части окна.
4. На закладке **Пользователи** установите флажки напротив тех пользователей, у которых вы хотите отозвать роль.
5. Нажмите на кнопку **Отозвать роль**.
6. В окне подтверждения нажмите на кнопку **Да**.

Роль будет отозвана у пользователя. Пользователь больше не сможет совершать действия с параметрами программы, которые были ему доступны в соответствии с правами этой роли.

kaspersky

Хранилище

Хранилище предназначено для копий сообщений, которые Kaspersky Secure Mail Gateway сохраняет во время обработки. Права доступа к копиям сообщений в Хранилище ограничены в целях обеспечения безопасности сервера Kaspersky Secure Mail Gateway.

Если к сообщению применяется правило, в параметрах которого установлен флажок **Поместить копию в Хранилище**, то, независимо от заданного действия, перед его выполнением программа помещает в Хранилище копию сообщения.

Копии сообщений помещаются в Хранилище вместе с вложениями.

Администратор программы может выполнять следующие действия с копиями сообщений в Хранилище при наличии соответствующих прав (см. раздел "Добавление роли" на стр. 139):

- Фильтровать сообщения в Хранилище (см. раздел "Фильтрация и поиск копий сообщений в Хранилище" на стр. 153).
- Просматривать информацию о сообщении (см. раздел "Просмотр информации о сообщении в Хранилище" на стр. 158) и результатах его обработки.
- Доставлять сообщения из Хранилища (см. раздел "Доставка сообщения из Хранилища" на стр. 160).
- Скачивать копии сообщений (см. раздел "Скачивание сообщения из Хранилища" на стр. 161) на компьютер.

  > Недоступно для персонального Хранилища.

- Удалять копии сообщений (см. раздел "Удаление копии сообщения из Хранилища" на стр. 162) из Хранилища.

  > При удалении из персонального Хранилища копия сообщения не удаляется из общего Хранилища. Все операции с копией этого сообщения остаются доступны в общем Хранилище.

По умолчанию максимальный объем Хранилища составляет 7 ГБ. Как только объем Хранилища превышает заданное по умолчанию пороговое значение, программа начинает удалять из Хранилища самые старые копии сообщений. Когда объем Хранилища снова становится меньше порогового значения, программа прекращает удалять копии сообщений из Хранилища.

В режиме администратора отображается информация обо всех копиях сообщений, помещенных в Хранилище. В режиме пользователя отображается персональное Хранилище с информацией о сообщениях только текущего пользователя.

> Просмотр персонального Хранилища, а также действия с копиями сообщений доступны пользователю, если администратор включил соответствующие опции в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 152).

kaspersky

В этом разделе

Настройка параметров Хранилища

► *Чтобы настроить параметры Хранилища:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Хранилище**.
2. В поле **Максимальный размер Хранилища (МБ)** укажите суммарный размер всех сообщений в Хранилище, при достижении которого более старые копии сообщений будут удаляться.

   Возможные значения – целые числа от 1024 до 2147483647 МБ (~2 ПБ). Значение по умолчанию – 7168 МБ (7 ГБ).
3. В поле **Срок хранения (дней)** укажите количество дней, по истечение которых более старые копии сообщений будут удаляться.

   Возможные значения – целые числа от 1 до 1100 (~ 3 года). Значение по умолчанию – 30 дней.

   > Копии сообщений удаляются согласно ограничению, которое достигается первым.
4. Выберите действие для сообщений, копии которых требуется поместить в Хранилище, если Хранилище недоступно:
   - **Продолжать обработку**.

     Сообщение будет обработано независимо от возможности помещения его копии в Хранилище. Если задано действие **Удалить вложение** или **Вылечить**, то измененное сообщение будет отправлено получателям после лечения или удаления вложения. Если задано действие **Удалить сообщение**, то сообщение будет удалено без уведомления отправителя. Если задано действие **Отклонить**, то сообщение будет отклонено.
   - **Сообщать о временной ошибке сервера**.

     Если при помещении копии сообщения в Хранилище произойдет ошибка, программа вернет SMTP-ошибку 451.
   - **Отклонять сообщения**.

     Если при помещении копии сообщения в Хранилище произойдет ошибка, сообщение будет отклонено.

5. Нажмите на кнопку **Сохранить**.

Параметры Хранилища будут настроены.

Настройка параметров персонального Хранилища

► *Чтобы настроить параметры персонального Хранилища:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Персональные учетные записи**.
2. Выберите закладку **Хранилище**.
3. Если вы хотите, чтобы в режиме пользователя отображался раздел персонального Хранилища с информацией о копиях помещенных в него сообщений, переведите переключатель **Просматривать информацию о сообщении** в положение **Включено**.
4. Если вы хотите, чтобы в режиме пользователя было доступно удаление сообщений из персонального Хранилища, переведите переключатель **Удалять сообщения** в положение **Включено**.
5. Если вы хотите, чтобы в режиме пользователя была доступна доставка безопасных сообщений из персонального Хранилища, переведите переключатель **Доставлять сообщения** в положение **Включено**.
6. В раскрывающемся списке ниже выберите, в каком формате следует доставлять сообщения из персонального Хранилища:
   - **во вложении**.
   - **в исходном виде**.
7. Нажмите на кнопку **Сохранить**.

Параметры персонального Хранилища будут настроены.

Просмотр таблицы объектов в Хранилище

Сообщения, к которым были применены действия **Пропустить** или **Отклонить** не помещаются в персональное Хранилище. Информация о таких сообщениях доступна только в Хранилище в режиме администратора.

► *Чтобы просмотреть таблицу объектов в Хранилище,*

в окне веб-интерфейса программы выберите раздел **Хранилище**.

В таблице отображается следующая информация об объектах в Хранилище:

- **Email отправителя** – адрес отправителя сообщения.
- **Email получателя** – адреса получателей сообщения.

> В персональном Хранилище информация о получателях из поля BCC не отображается.

- **Тема** – тема сообщения.
- **Причина помещения** – название модуля программы, согласно параметрам которого сообщение было помещено в Хранилище.
- **Размер сообщения** – размер сообщения.
- **Время получения** - дата и время получения сообщения.
- **App ID сообщения** – уникальный идентификатор, присваиваемый сообщению программой.
- **SMTP message ID** – идентификатор, присваиваемый сообщению на почтовом сервере.
- **Узел** – IP-адрес узла кластера, на котором было обработано сообщение.

  Графа недоступна в персональном Хранилище.

> По умолчанию в таблице отображаются не все графы. Вы можете настроить отображение таблицы (см. раздел "Настройка отображения таблицы объектов в Хранилище" на стр. 153).

Настройка отображения таблицы объектов в Хранилище

► *Чтобы настроить отображение таблицы объектов в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

   Откроется таблица объектов Хранилища.

2. По кнопке **Настроить таблицу** откройте меню отображения таблицы.
3. Установите флажки рядом с теми параметрами, которые должны отображаться в таблице.

   > Должен быть установлен хотя бы один флажок.

Отображение таблицы объектов Хранилища будет настроено.

Фильтрация и поиск копий сообщений в Хранилище

► *Чтобы найти копии сообщений в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
2. Нажмите на кнопку .

Откроется окно **Фильтры**.

3. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска копий сообщений.
4. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Технология обнаружения	Для этого критерия логические операторы не предусмотрены.	Установите флажки рядом с названиями модулей программы, по результатам проверки которыми сообщения были помещены в Хранилище. Вы можете выбрать один или несколько модулей проверки: • **Антивирус**. • **Анти-Спам**. • **Анти-Фишинг**. • **Контентная фильтрация**. • **Пользовательский список запрещенных адресов**. • **Проверка ссылок**. • **Проверка подлинности отправителей**. • **KATA** (отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228)).
Email отправителя	• **включает**.	Текст поиска адресов электронной почты отправителей сообщений. Вы можете ввести адрес электронной почты (например, example-email@example.com), имя домена (например, example.com) или несколько символов из адреса электронной почты (например, exa). Если вы настроили интеграцию с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 224), программа будет искать записи в LDAP-кеше, совпадающие с введенной строкой поиска, и отображать подсказку с именами учетных записей.
IP отправителя	• **равно**.	Текст поиска IP-адреса, с которого было отправлено сообщение. Вы можете ввести адрес в формате IPv4 или IPv6.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Email получателя	• **включает**.	Текст поиска адресов электронной почты получателей сообщений. Вы можете ввести адрес электронной почты (например, example-email@example.com), имя домена (например, example.com) или несколько символов из адреса электронной почты (например, exa). Если вы настроили интеграцию с LDAP-сервером (см. раздел "Интеграция с внешней службой каталогов" на стр. 224), программа будет искать записи в LDAP-кеше, совпадающие с введенной строкой поиска, и отображать подсказку с именами учетных записей. При фильтрации сообщений в персональном Хранилище адреса получателей из поля BCC не учитываются.
Тема	• **включает**.	Текст поиска заголовков сообщений
App ID сообщения	• **равно**.	Уникальный идентификатор, присвоенный сообщению программой.
SMTP message ID	• **включает**.	Идентификатор сообщения на почтовом сервере. Этот идентификатор может быть использован для поиска сообщения в Хранилище при обращении пользователей, если вы настроили добавление идентификатора в уведомления об отклоненных сообщениях (см. раздел "Добавление в уведомление уникального идентификатора сообщения" на стр. 268).

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Дата и время	• **после**. • **до**.	Интервал обработки сообщений и помещения их копий в Хранилище.
Размер сообщения (КБ)	• **больше или равно**. • **меньше или равно**.	Ограничение поиска по размеру сообщений в килобайтах.
Узел	• **равно**. • **не равно**.	Узел кластера, на котором было обработано сообщение. Критерий недоступен в персональном Хранилище.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку **Добавить фильтр**.

5. Нажмите на кнопку **Применить**.

Копии сообщений, удовлетворяющие параметрам поиска, отобразятся в списке копий сообщений в разделе **Хранилище**.

В таблице отображается информация о последних 5000 сообщений. Если согласно заданным критериям фильтрации найдено более 5000 сообщений, рекомендуется уточнить критерии поиска.

Просмотр информации о сообщении в Хранилище

► *Чтобы просмотреть информацию о сообщении в Хранилище, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
2. В таблице объектов Хранилища выберите сообщение, информацию о котором вы хотите посмотреть.

   Откроется окно **Просмотреть информацию о сообщении**.

В окне содержится следующая информация о сообщении:

- **Причина**.

  Название модуля программы, по результатам проверки которого сообщение было помещено в Хранилище.

- **App ID сообщения**.

  Уникальный идентификатор, присваиваемый сообщению программой в процессе обработки.

- **Тема**.

  Тема сообщения.

- **Email отправителя**.

  Адрес электронной почты отправителя сообщения.

- **IP отправителя**.

  IP-адрес сервера, с которого было отправлено сообщение.

- **Отправлено**.

  Дата и время отправки сообщения.

- **Получено**.

  Дата и время получения сообщения программой для начала его обработки.

- **Узел**.

  Узел, на котором было обработано сообщение.

  > Поле недоступно в персональном Хранилище.

- **SMTP message ID**.

  Идентификатор, присвоенный сообщению почтовым сервером.

- **Вложения**.

  Имена и размеры вложений (в байтах).

- Раздел **Правила**, содержащий следующую информацию о правилах, согласно которым копия сообщения была помещена в Хранилище:

  - Название правила.
  - **Email получателя**.

    Адреса электронной почты получателей из поля `To`.

  - **CC**.

    Адреса электронной почты получателей из поля `CC`.

  - **BCC**.

    Адреса электронной почты получателей из поля `BCC`.

    > Поле недоступно в персональном Хранилище.

  - **Действие**.

    Действие, которое было выполнено над сообщением по результатам проверки всеми модулями программы.

  - **Результат проверки**.

    Вы можете развернуть этот блок и просмотреть детальную информацию о результатах проверки по каждому модулю программы.

    - **Антивирус**.
    - **Анти-Спам**.
    - **Анти-Фишинг**.

- **Проверка ссылок**.
- **Контентная фильтрация**.
- **Персональный список запрещенных адресов**.
- **Подлинность отправителей**.

  Вы можете развернуть этот блок и просмотреть детальную информацию о результатах проверки по каждой из технологий: SPF, DKIM, DMARC.

- **KATA**.

  Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

- **Причина**.

  Название модуля программы, по результатам проверки которого сообщение было помещено в Хранилище.

- Блок параметров **Доставить сообщение**, позволяющих отправить сообщение получателям или переслать его на другие адреса во вложении или в исходном виде.

  Блок недоступен в персональном Хранилище. В режиме администратора блок отображается только при наличии разрешений на отправку сообщений из Хранилища (см. раздел "Работа с ролями и учетными записями пользователей" на стр. 139).

По ссылке в верхней части окна с информацией о сообщении вы можете перейти в раздел **События** и посмотреть информацию о событиях, связанных с обработкой этого сообщения.

Доставка сообщения из Хранилища

В режиме администратора можно доставлять сообщения из общего Хранилища получателям или пересылать их на любые адреса. Доступные параметры доставки определяются наличием соответствующих прав (см. раздел "Добавление роли" на стр. 139).

В режиме пользователя можно доставлять сообщения из персонального Хранилища на адрес текущего пользователя, если администратор включил эту опцию в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 152). Доставка небезопасных сообщений из персонального Хранилища недоступна.

При доставке сообщения из персонального Хранилища удаляется информация о получателях из поля BCC.

► *Чтобы доставить сообщение из общего Хранилища:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
2. В таблице объектов Хранилища выберите сообщение, которое вы хотите доставить.

   Откроется окно **Просмотреть информацию о сообщении**.

3. Если вы хотите доставить сообщение получателям, выполните следующие действия:

a. Включите переключатель **На адреса электронной почты получателей, чьи сообщения были помещены в Хранилище**.

b. Установите флажки напротив адресов тех получателей, которым вы хотите доставить сообщение.

4. Если вы хотите переслать сообщение на другие адреса, выполните следующие действия:

a. Включите переключатель **На дополнительные адреса электронной почты**.

b. В поле ввода ниже укажите адреса электронной почты, на которые вы хотите переслать сообщение.

5. Установите флажок рядом с названием параметра **Доставить сообщение в виде вложения**, если вы хотите доставить сообщение в виде вложения.

Если флажок снят, сообщение будет отправлено в исходном виде.

По умолчанию флажок установлен.

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от программы" на стр. 269), который указывается в качестве отправителя сообщения, содержащего вложение из Хранилища.

6. Нажмите на кнопку **Доставить**.

7. В окне подтверждения нажмите на кнопку **ОК**.

Сообщение будет помещено в очередь на доставку.

► *Чтобы доставить сообщение из персонального Хранилища:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

2. В таблице объектов Хранилища выберите сообщение, которое вы хотите доставить.

Откроется окно **Просмотреть информацию о сообщении**.

3. Нажмите на кнопку **Доставить** в правом нижнем углу.

4. В окне подтверждения нажмите на кнопку **ОК**.

Сообщение будет помещено в очередь на доставку. Сообщение будет доставлено в формате, заданном администратором в параметрах персонального Хранилища (см. раздел "Настройка параметров персонального Хранилища" на стр. 152).

Скачивание сообщения из Хранилища

Скачивание сообщений из персонального Хранилища недоступно.

► *Чтобы скачать сообщение из Хранилища:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.

2. В таблице объектов Хранилища выберите сообщение, которое вы хотите сохранить на жесткий диск.

Откроется окно **Просмотреть информацию о сообщении**.

3. В правом нижнем углу окна нажмите на кнопку **Скачать**.

Сообщение будет сохранено в папке загрузки браузера.

Удаление копии сообщения из Хранилища

При удалении из персонального Хранилища копия сообщения не удаляется из общего Хранилища. Все операции с копией этого сообщения остаются доступны в общем Хранилище.

► *Чтобы удалить копию сообщения из Хранилища, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Хранилище**.
2. В таблице объектов Хранилища выберите сообщение, копию которого вы хотите удалить.

   Откроется окно **Просмотреть информацию о сообщении**.
3. Нажмите на кнопку **Удалить** в правом нижнем углу.
4. В окне подтверждения нажмите на кнопку **ОК**.

Копия сообщения будет удалена из Хранилища.

kaspersky

Журнал событий Kaspersky Secure Mail Gateway

Во время работы Kaspersky Secure Mail Gateway возникают различного рода события. Они отражают изменение состояния программы. Для того, чтобы администратор программы мог самостоятельно проанализировать ошибки, допущенные при настройке параметров программы, а также для того, чтобы специалисты "Лаборатории Касперского" могли оказать эффективную техническую поддержку, Kaspersky Secure Mail Gateway записывает информацию об этих событиях в *журнал событий*.

Журнал событий хранится на узлах программы. Записи в журнале событий автоматически ротируются по достижении максимально разрешенного размера файлов или по истечении максимального срока их хранения.

Программа распределяет события по следующим уровням:

- **Ошибка** – сообщения об ошибках в работе программы.
- **Информация** – информационные сообщения.

В этом разделе

Просмотр журнала событий

► *Чтобы просмотреть журнал событий Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**
   - **Система**.

   Информация о событиях отобразится в виде таблицы.

   В графах таблицы событий обработки почтового трафика отображается следующая информация:
   - **Дата и время** – дата и время выполнения события.

- **Email отправителя** – имя отправителя сообщения.
- **Email получателя** – имя получателя сообщения.
- **Тема** – тема сообщения.
- **Название правила** – название правила, в соответствии с которым было обработано сообщение.

  Вы можете просмотреть подробную информацию о правиле, нажав на ссылку с названием правила.
- **Действие** – действие, выполненное над сообщением.
- **Узел** – IP-адрес и порт узла, на котором было обработано сообщение.

В графах таблицы системных событий отображается следующая информация:

- **Дата и время** – дата и время выполнения события.
- **Узел** – IP-адрес и порт узла, на котором было обработано сообщение.
- **Тип события** – тип события.
- **Имя пользователя** – имя пользователя узла, на котором произошло событие.
- **Результат** – результат обработки события.
- **Сведения** – название детектирующей технологии, в соответствии с которой было записано событие.

3. Вы можете сортировать события в графах. Для этого нажмите на название графы в таблице:
   - События в графах **Email отправителя**, **Email получателя**, **Тема**, **Название правила**, **Действие**, **Тип события**, **Имя пользователя**, **Результат**, **Сведения** сортируются по алфавиту в порядке A–Z и Z–A.

     По умолчанию записи о событиях отображаются по алфавиту в порядке A–Z.
   - События в графах **Дата и время** и **Узел** сортируются в порядке возрастания и убывания.

     По умолчанию записи о событиях отображаются в порядке возрастания.

Отобразится таблица событий, удовлетворяющих условиям сортировки.

Настройка отображения таблицы событий

► *Чтобы настроить отображение таблицы событий, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**
   - **Система**.

   Информация о событиях отобразится в виде таблицы.
3. Нажмите на кнопку  .

   Отобразится окно **Настроить таблицу**.

4. Если вы хотите включить / отключить отображение графы в таблице, выполните следующие действия:
   - Если вы хотите включить отображение графы в таблице, установите флажок рядом с тем параметром, который должен отображаться в таблице. Вы можете выбрать сразу несколько параметров.
   - Если вы хотите отключить отображение графы в таблице, снимите флажок рядом с тем параметром, который не должен отображаться в таблице. Вы можете выбрать сразу несколько параметров.

   > Должен быть установлен хотя бы один флажок.

5. Если вы хотите изменить порядок отображения граф в таблице, выполните следующие действия:
   a. Выберите строку с нужным параметром.
   b. Нажмите на кнопку со значком вверх / вниз в правом нижнем углу окна.
6. Закройте окно настройки вида таблицы.

Отображение таблицы событий будет настроено.

Фильтрация событий обработки почтового трафика

Вы можете отфильтровать события в журнале событий по одному или нескольким критериям.

► *Чтобы отфильтровать события обработки почтового трафика в журнале событий, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Почтовый трафик**.

   Информация о событиях отобразится в виде таблицы.
3. Нажмите на кнопку **Фильтры**.

   Отобразится окно добавления фильтра.
4. Нажмите на кнопку **Добавить фильтр**.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Дата и время	• **после**. • **до**.	Интервал обработки сообщений.
Email отправителя	• **включает**. • **не включает**. • **равно**. • **не равно**.	Текст поиска адресов электронной почты отправителей сообщений. Вы можете ввести адрес электронной почты (например, example-email@example.com), имя домена (например, example.com) или несколько символов из адреса электронной почты (например, exa).
Email получателя	• **включает**. • **не включает**. • **равно**. • **не равно**.	Текст поиска адресов электронной почты получателей сообщений.
Тема	• **включает**. • **не включает**.	Текст поиска заголовков сообщений
Название правила	• **включает**. • **не включает**. • **равно**. • **не равно**.	Название правила, которое было применено при обработке сообщения.
Действие	• **равно**. • **не равно**.	Действие, выполненное над сообщением.
IP отправителя	• **равно**. • **не равно**.	Текст поиска IP-адреса, с которого было отправлено сообщение. Вы можете ввести адрес в формате IPv4 или IPv6.
App ID сообщения	• **равно**. • **не равно**.	Уникальный идентификатор, присвоенный сообщению программой.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
SMTP message ID	• **включает**. • **не включает**. • **равно**. • **не равно**.	Идентификатор сообщения на почтовом сервере. Этот идентификатор может быть использован для поиска события при обращении пользователей, если вы настроили добавление идентификатора в уведомления об отклоненных сообщениях (см. раздел "Добавление в уведомление уникального идентификатора сообщения" на стр. 268).
Узел	• **равно**. • **не равно**.	Узел кластера, на котором было обработано сообщение.
Статус проверки В раскрывающемся списке справа выберите одну из следующих технологий обнаружения: • **Анти-Фишинг**. • **Анти-Спам**. • **Антивирус**. • **Контентная фильтрация**. • **Проверка подлинности отправителей**. • **Проверка ссылок**. • **KATA** (отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228)).	• **включает**. • **не включает**.	Нажмите на поле **Выбрать статусы** и в раскрывшемся списке установите флажки напротив статусов, по которым вы хотите отфильтровать события. Набор отображаемых статусов зависит от выбранной технологии.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку **Добавить фильтр**.

6. Нажмите на кнопку **Найти**.
7. Закройте окно добавления фильтра.

Отобразится таблица событий, удовлетворяющих критериям фильтрации.

В таблице отображается информация о последних 5000 событий. Если согласно заданным критериям фильтрации найдено более 5000 событий, рекомендуется уточнить критерии поиска.

kaspersky

Фильтрация системных событий

Информация о системных событиях записывается в журнал событий узла, на котором произошли события. При удалении узла из кластера или потери доступа к узлу журнал событий будет недоступен.

Вы можете отфильтровать события в журнале событий по одному или нескольким критериям.

► *Чтобы отфильтровать системные события в журнале событий, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Система**.

   Информация о событиях отобразится в виде таблицы.
3. Нажмите на кнопку **Фильтры**.

   Отобразится окно добавления фильтра.
4. Нажмите на кнопку **Добавить фильтр**.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Дата и время	• **после**; • **до**.	Интервал времени, в который произошло событие.
Узел	• **равно**; • **не равно**.	IP-адрес и порт узла, на котором произошло событие.
Тип события	• **равно**; • **не равно**.	Выберите один из следующих типов события: • **Синхронизация LDAP**; • **Аудит**; • **Обновление баз**; • **Экспорт параметров**; • **Импорт параметров**.
Имя пользователя	• **включает**; • **не включает**; • **равно**; • **не равно**.	Имя пользователя в LDAP, под учетной записью которого произошло событие. Действия, выполненные программой автоматически, записываются в журнал событий под учетной записью пользователя kluser.
Результат	• **равно**; • **не равно**.	Выберите один из следующих вариантов: • **Успешно**; • **Ошибка**.

Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку **Добавить фильтр**.

6. Нажмите на кнопку **Найти**.
7. Закройте окно добавления фильтра.

Отобразится таблица событий, удовлетворяющих критериям фильтрации.

В таблице отображается информация о последних 5000 событий. Если согласно заданным критериям фильтрации найдено более 5000 событий, рекомендуется уточнить критерии поиска.

Просмотр информации о событии обработки почтового трафика

По ссылке в верхней части окна вы можете перейти в раздел **Хранилище** и посмотреть информацию о сообщениях в Хранилище, связанных с этим событием.

► *Чтобы просмотреть информацию о событии обработки почтового трафика, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите закладку **Почтовый трафик**.

   Информация о событиях обработки почтового трафика отобразится в виде таблицы.
3. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии.

В окне с информацией о событии обработки почтового трафика отображаются следующие поля:

- **Дата и время** – дата и время выполнения события.
- **Узел** – IP-адрес и порт узла, на котором было обработано сообщение.
- **Email отправителя** – имя отправителя сообщения.
- **Кому** – имя получателя сообщения.
- **CC** – имя получателя копии сообщения.
- **BCC** – имя получателя скрытой копии сообщения.
- **Тема** – тема сообщения.
- **Название правила** – название правила, в соответствии с которым было обработано сообщение.

  Вы можете просмотреть подробную информацию о правиле, нажав на ссылку с названием правила.
- **Действие** – действие, выполненное над сообщением.
- Блок параметров **Результат проверки**, в котором отображаются статусы, присвоенные сообщению каждым модулем проверки.
  - **Антивирус**:
    - *Не проверено*.
    - *Не обнаружено*.
    - *Зашифровано*.
    - *Ошибка*.
    - *Вылечено*.
    - *Заражено*.
  - **Анти-Спам**:
    - *Не проверено*.
    - *Не обнаружено*.
    - *Доверенный источник*.
    - *Формальное сообщение*.
    - *Ошибка*.
    - *Предполагаемый спам*.
    - *В списке запрещенных адресов*.

- *Спам*.
- *Массовая рассылка*.

- **Анти-Фишинг**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Ошибка*.
  - *Фишинг*.
- **Проверка ссылок**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Ошибка*.
  - *Обнаружено*.
  - *Ошибка баз*.
- **Контентная фильтрация**:
  - *Не проверено*.
  - *Не обнаружено*.
  - *Превышен допустимый размер*.
  - *Запрещенное имя вложения*.
  - *Запрещенный формат вложения*.
  - *Ошибка*.
- **KATA**:
  - *Обнаружено*.
  - *Ошибка*.
  - *Не обнаружено*.
  - *Не проверено*.
  - *Пропущено*.

  Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

- Информация о вложении:
  - **Имя файла**.
  - **Размер файла (в байтах)**.
  - **Формат файла**.

    Информация о формате файла отображается, если формат вложенного файла был указан в правиле обработки контентной фильтрации (см. раздел "Настройка контентной фильтрации" на стр. 111).
- Результат проверки вложения.

kaspersky

Типы системных событий

Описание системных событий, информация о которых записывается в журнал событий (раздел **События** → **Система**), представлено в таблице ниже.

Таблица 4. Описание системных событий разных типов

Тип события	Результат обработки события	Сведения
Обновление баз	Успешно	Антивирусные базы актуальны
	Успешно	Обновление запущено
	Успешно	Антивирусные базы применены. Время обновления: "<Дата и время обновления>"
	Ошибка	Ошибка обновления баз:<Название ошибки>
	Ошибка	Ошибка загрузки антивирусных баз: <Название ошибки>
	Успешно	Базы Анти-Спама актуальны
	Успешно	Базы Анти-Спама применены. Время обновления: "<Дата и время обновления>"
	Ошибка	Ошибка загрузки баз Анти-Спама: <Название ошибки>
	Успешно	Базы Анти-Фишинга актуальны
	Успешно	Базы Анти-Фишинга применены. Время обновления: "<Дата и время обновления>"
	Ошибка	Ошибка загрузки баз Анти-Фишинга: <Название ошибки>
Аудит	Успешно	Аудит запущен
Синхронизация LDAP	Успешно	Запущена синхронизация LDAP
Экспорт параметров	Ошибка	Экспорт параметров программы завершился с ошибкой
	Успешно	Параметры программы экспортированы
Импорт параметров	Ошибка	Импорт параметров программы завершился с ошибкой
	Успешно	Параметры программы импортированы

kaspersky

Экспорт журнала событий

Вы можете экспортировать таблицу событий в файл формата CSV.

► *Чтобы экспортировать таблицу событий, выполните следующие действия:*

1. В окне веб-интерфейса программы в дереве консоли управления выберите раздел **События**.
2. Выберите одну из следующих закладок в зависимости от типа событий, которые вы хотите просмотреть:
   - **Почтовый трафик.**
   - **Система**.

   Информация о событиях отобразится в виде таблицы.
3. Нажмите на кнопку **Экспорт**.
4. Если откроется окно выбора файла, укажите путь, по которому должен быть сохранен файл, и нажмите на кнопку **Save**.

   В некоторых браузерах файл автоматически сохраняется в папку загрузки браузера без возможности выбрать другой путь.

Начнется загрузка файла. Таблица событий будет экспортирована в файл формата CSV.

Если вы предварительно отфильтровали события в таблице (см. раздел "Фильтрация событий обработки почтового трафика" на стр. 165), настроили сортировку событий в графах (см. раздел "Просмотр журнала событий" на стр. 163) и отображение граф в таблице (см. раздел "Настройка отображения таблицы событий" на стр. 164), все заданные настройки сохранятся при экспорте таблицы в файл.

Настройка параметров журнала событий

При настройке длительности хранения событий и выборе типов событий для записи необходимо учитывать доступное дисковое пространство на обрабатывающих серверах.

Параметры записи событий в журнал событий не влияют на параметры записи событий по протоколу Syslog.

► *Чтобы настроить параметры записи в журнал событий, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Журналы и события** → **События**.
2. В блоке параметров **Почтовый трафик** выполните следующие действия:

a. В раскрывающемся списке **Записывать события обработки трафика** выберите, какие события обработки трафика должны быть записаны в журнал событий. Вы можете выбрать один из следующих вариантов:

- **Все**;
- **Применено действие Удалить сообщение/Удалить вложение/Отклонить**;
- **Не записывать**.

По умолчанию выбран параметр **Все**.

> Новые настройки параметра применяются только к событиям, записанным в журнал событий после применения настроек. К событиям, которые были записаны в журнал ранее, новые настройки не применяются.
> Настройки параметра применяются на всех узлах кластера.

b. В поле **Максимальный размер журнала событий (МБ)** укажите размер журнала событий, при превышении которого более старые записи будут удалены.

Значение по умолчанию: 1024 МБ.

c. В поле **Срок хранения событий в журнале (дней)** укажите, сколько дней программа должна хранить события обработки сетевого трафика на сервере.

Значение по умолчанию: 3 дня.

3. В блоке параметров **Система** в поле **Максимальное количество событий** укажите количество записей о событиях Kaspersky Secure Mail Gateway, при превышении которого более старые записи будут удалены.

Значение по умолчанию: 100 тыс.

Параметры записи событий в журнал событий будут настроены.

kaspersky

Очередь сообщений

Этот раздел содержит информацию о работе с очередями сообщений Kaspersky Secure Mail Gateway, а также о том, как отсортировать, отфильтровать, принудительно отправить сообщения из очереди сообщений, а также Анти-Спам карантина и KATA карантина или выполнить поиск сообщений в очереди.

В этом разделе

Просмотр таблицы сообщений в очереди

► *Чтобы просмотреть таблицу сообщений в очереди,*

в окне веб-интерфейса программы выберите раздел **Очередь сообщений**.

В таблице отображается следующая информация о сообщениях в очереди:

- **Очередь**.
- **ID сообщения**.
- **Email отправителя**.
- **Email получателя**.
- **Тема**.
- **Размер сообщения**.
- **Время получения**.
- **Ошибка**.
- **Узел**.

kaspersky

Включение и отключение отправки и приема сообщений

► *Чтобы включить или отключить отправку или прием сообщений почтовым агентом Kaspersky Secure Mail Gateway, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Очередь сообщений**.
2. Нажмите на кнопку **Настроить параметры приема и отправки**.

   Откроется окно **Параметры приема и отправки**.
3. В раскрывающемся списке **Выбрать узел** выберите узел, для которого вы хотите настроить прием или отправку сообщений.

   Если вы хотите применить параметры сразу ко всем узлам кластера, выберите **Все узлы**.
4. Включите или отключите прием сообщений с помощью переключателя **Прием**.
5. Включите или отключите отправку сообщений с помощью переключателя **Отправка**.

   Если в расширенных параметрах MTA (см. раздел "Настройка расширенных параметров MTA" на стр. 279) установлен параметр **Отклонять сообщения на неизвестные домены** (reject_unverified_recipient), прием сообщений также будет отключен.

Внимание! Эти параметры определяют отправку и прием сообщений почтовым агентом Kaspersky Secure Mail Gateway.

Просмотр сводной статистики

Информация о KATA карантине отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

► *Чтобы просмотреть сводную статистику по всем узлам кластера,*

в окне веб-интерфейса программы выберите раздел **Очередь сообщений**.

Отобразится следующая информация:

- **Очередь MTA, занято**. Суммарный размер сообщений во всех очередях Postfix и процент занимаемого дискового пространства.
- **Очередь MTA, сообщений**. Общее количество сообщений во всех очередях Postfix в настоящий момент.

- **Анти-Спам карантин, занято**. Размер Анти-Спам карантина и процент использования Анти-Спам карантина по сравнению с максимальным размером, заданным в параметрах модуля Анти-Спам (см. стр. 206).
- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине в настоящий момент.
- **KATA карантин, занято**. Размер KATA карантина и процент использования KATA карантина по сравнению с максимальным размером, заданным в параметрах защиты KATA (см. раздел "Настройка параметров защиты KATA" на стр. 229).
- **KATA карантин, сообщений**. Количество сообщений в KATA карантине в настоящий момент.

Вы также можете просмотреть статистику по каждому узлу кластера отдельно (см. раздел "Просмотр статистики по узлам" на стр. 178).

Просмотр статистики по узлам

Информация о KATA карантине отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

► *Чтобы просмотреть статистику по узлам кластера:*

1. В веб-интерфейсе программы выберите раздел **Очередь сообщений**.
2. Нажмите на кнопку **Показать статистику очередей по узлам**.

   Откроется страница **Статистика очередей по узлам**.

На странице отображается таблица со статистикой очередей по узлам кластера. Таблица содержит следующие графы:

- **Узел**. IP-адрес и порт подключения к узлу кластера.
- **Очередь MTA, сообщений**. Общее количество сообщений во всех очередях Postfix в настоящий момент.
- **Очередь MTA, занято**. Суммарный размер сообщений во всех очередях Postfix.
- **Очередь MTA, занято (%)**. Процент дискового пространства, занимаемого сообщениями всех очередей Postfix.
- **Анти-Спам карантин, сообщений**. Количество сообщений в Анти-Спам карантине в настоящий момент.
- **Анти-Спам карантин, занято**. Размер Анти-Спам карантина.
- **Анти-Спам карантин, занято (%)**. Процент использования Анти-Спам карантина по сравнению с максимальным размером, заданным в параметрах модуля Анти-Спам (см. стр. 206).
- **KATA карантин, сообщений**. Количество сообщений в KATA карантине в настоящий момент.
- **KATA карантин, занято**. Размер KATA карантина.
- **KATA карантин, занято (%)**. Процент использования KATA карантина по сравнению с максимальным размером, заданным в параметрах защиты KATA (см. раздел "Настройка параметров защиты KATA" на стр. 229).

Если в очередях более 5000 сообщений, отображается примерное их количество.

Сортировка сообщений в очереди

► Чтобы отсортировать *сообщения в очереди*, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Очередь сообщений**.

   Откроется таблица сообщений в очереди.
2. Нажмите на название той графы таблицы, по которой вы хотите отсортировать сообщения:
   - **Очередь** – название очереди.
   - **ID сообщения** – ID сообщений в очереди.
   - **Email отправителя** – адрес отправителя сообщений.
   - **Email получателя** – адрес получателя сообщений.
   - **Тема** – тема сообщения.
   - **Размер сообщения** – размер сообщений.
   - **Время получения** – время поступления сообщений в очередь.
   - **Ошибка** – ошибка проверки сообщений.
   - **Узел** – узел кластера, на котором было обработано сообщение.
3. Если вы хотите изменить порядок сортировки, нажмите на название графы повторно. Слева от названия графы отобразится новый порядок сортировки в виде кнопки или .

Сообщения в очереди будут отсортированы.

Фильтрация и поиск сообщений в очереди

► Чтобы отфильтровать или найти сообщения в *очереди*, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Очередь сообщений**.
2. Нажмите на кнопку **Фильтры**.

   Откроется окно **Фильтры**.
3. В блоке параметров **Очередь** установите флажки рядом с названиями очередей, по которым вы хотите отфильтровать сообщения.

   Вы можете выбрать одну или несколько очередей:
   - **KATA-карантин**.
   - **Анти-Спам карантин**.
   - **Deffered**.
   - **Hold**.

- **Active**.
- **Inbound**.

  Очередь Inbound содержит сообщения из очередей Incoming и Maildrop.

4. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска сообщения.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Email отправителя	• **включает**.	Текст поиска адресов электронной почты отправителей сообщений. Вы можете ввести адрес электронной почты (например, example-email@example.com), имя домена (например, example.com) или несколько символов из адреса электронной почты (например, exa).
Email получателя	• **включает**.	Текст поиска адресов электронной почты получателей сообщений.
Дата сообщения	• **после**; • **до**.	Интервал обработки сообщений и помещения их копий в Хранилище.
Размер сообщения (КБ)	• **меньше или равно**; • **больше или равно**.	Ограничение поиска по размеру сообщений в килобайтах.
ID сообщения	• **включает**.	Уникальный идентификатор, присвоенный сообщению программой.
Узел	• **равно**; • **не равно**.	Узел кластера, на котором было обработано сообщение.

   Вы можете указать несколько критериев фильтрации. Для добавления еще одного критерия необходимо нажать на кнопку  .

6. Нажмите на кнопку **Применить**.

Копии сообщений, удовлетворяющие параметрам поиска, отобразятся в списке сообщений в разделе **Очередь сообщений**.

В таблице отображается информация о последних 5000 сообщений. Если согласно заданным критериям фильтрации найдено более 5000 сообщений, рекомендуется уточнить критерии поиска.

kaspersky

Принудительная отправка сообщений из очереди

Принудительная отправка сообщений из Анти-Спам карантина может привести к снижению уровня обнаружения спама.

Частые попытки вне очереди отправить недоставленные сообщения ухудшают скорость отправки остальных сообщений.

Чтобы принудительно отправить сообщения из очереди, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Очередь сообщений**.
2. Установите флажки рядом с сообщениями, которые вы хотите отправить, или выделите все сообщения.
3. В панели инструментов в верхней части рабочей области нажмите на кнопку **Отправить**.

   Если вы выделили все сообщения и установили критерии фильтрации, то операция применяется только к сообщениям, удовлетворяющим заданным критериям. При необходимости отправить все сообщения в очереди требуется сбросить фильтр.
4. В окне подтверждения выполните одно из следующих действий:
   - Если количество сообщений менее 5000, нажмите на кнопку **ОК**, чтобы подтвердить принудительную отправку всех сообщений (выбранных или удовлетворяющих заданным критериям фильтрации).
   - Если количество сообщений превышает 5000, выберите, требуется ли отправить только отображаемые сообщения или все сообщения (находящиеся во всех очередях или удовлетворяющие заданным критериям фильтрации).

Сообщения будут отправлены.

См. также

Удаление сообщений из очереди

► *Чтобы удалить сообщения из очереди, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Очередь сообщений**.
2. Установите флажки рядом с сообщениями, которые вы хотите удалить, или выделите все сообщения.
3. В панели инструментов в верхней части рабочей области нажмите на кнопку **Удалить**.

   Если вы выделили все сообщения и установили критерии фильтрации, то операция применяется только к сообщениям, удовлетворяющим заданным критериям. При необходимости удалить все сообщения в очереди требуется сбросить фильтр.

4. В окне подтверждения выполните одно из следующих действий:
   - Если количество сообщений менее 5000, нажмите на кнопку **ОК**, чтобы подтвердить удаление всех сообщений (выделенных или удовлетворяющих заданным критериям фильтрации).
   - Если количество сообщений превышает 5000, выберите, требуется ли удалить только отображаемые сообщения или все сообщения (находящиеся во всех очередях или удовлетворяющие заданным критериям фильтрации).

Сообщения будут удалены.

kaspersky

Отчеты

Для отслеживания результатов работы программы вы можете создавать отчеты.

Kaspersky Secure Mail Gateway поддерживает создание разовых отчетов по запросу пользователя (см. раздел "Создание отчета по требованию" на стр. 184), а также настройку регулярных отчетов, создаваемых по расписанию (см. раздел "Настройка параметров отчетов по расписанию" на стр. 185).

Информация обо всех созданных отчетах (см. раздел "Просмотр информации об отчете" на стр. 187) отображается в виде таблицы в разделе **Отчеты**. Для удобства поиска вы можете фильтровать и сортировать записи об отчетах (см. раздел "Фильтрация и сортировка отчетов" на стр. 186).

Чтобы ознакомиться с содержанием отчета (см. раздел "Содержание отчетов" на стр. 188), вы можете выполнить следующие действия:

- настроить отправку отчета по электронной почте во время его создания по требованию или при настройке расписания;
- переслать ранее созданный отчет на дополнительные адреса (см. раздел "Отправка отчетов по электронной почте" на стр. 193), а также повторно отправить на исходные адреса;
- скачать отчет на компьютер (см. раздел "Скачивание отчетов" на стр. 192).

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от программы" на стр. 269), который указывается в качестве отправителя отчетов о работе программы.

Отчеты хранятся в базе данных на Управляющем узле. Если вы назначите роль Управляющего узла в кластере другому серверу, все ранее созданные отчеты будут потеряны.

В этом разделе

kaspersky

Создание отчета по требованию

► *Чтобы создать отчет по требованию:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите закладку **По требованию**.
3. Нажмите на кнопку **Создать отчет**.

   Откроется окно **Создать отчет вручную**.
4. В раскрывающемся списке **Период** выберите тип временного интервала, за который вы хотите сформировать отчет:
   - **Другой** – любой временной интервал (доступны последние 124 дня).
   - **День** – с 00:00:00 до 23:59:59 выбранного дня (при выборе текущего дня – с 00:00:00 до момента создания отчета).

     Доступны последние 7 дней, включая текущий.
   - **Неделя** – с 00:00:00 понедельника до 23:59:59 воскресенья выбранной недели (при выборе текущей недели – с 00:00:00 понедельника до момента создания отчета).

     Доступны последние 17 недель, включая текущую.
   - **Месяц** – с 00:00:00 1 числа до 23:59:59 последнего дня выбранного месяца (при выборе текущего месяца – с 00:00:00 1 числа до момента создания отчета).

     Доступны последние 4 месяца, включая текущий.
   - **Год** – с 00:00:00 1 января до 23:59:59 31 декабря выбранного года (при выборе текущего года – с 00:00:00 1 января до момента создания отчета).

     Доступны последние 3 года, включая текущий.
5. Нажмите на текстовую область в поле ниже и в раскрывшемся календаре выберите временной интервал, данные за который должны быть представлены в отчете.
6. В раскрывающемся списке **Узлы** выберите адрес узла кластера, данные о котором вы хотите получить в отчете, или **Все узлы**, если вы хотите получить данные обо всех узлах.
7. Если вы хотите отправить созданный отчет по электронной почте, в блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится новый блок параметров доставки отчета.
8. В поле **Адреса электронной почты** введите адреса, на которые вы хотите отправить отчет.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.
9. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправить отчет.
10. В раскрывающемся списке **Язык** выберите язык отчета.
11. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка  справа от блока.
12. Нажмите на кнопку **Создать**.

Отчет будет создан. Информация об отчете (см. раздел "Просмотр информации об отчете" на стр. 187) отобразится в таблице на закладке **По требованию**. Вы можете скачать созданный отчет (см. раздел "Скачивание отчетов" на стр. 192) или отправить его по электронной почте (см. раздел "Отправка отчетов по электронной почте" на стр. 193).

Настройка параметров отчетов по расписанию

Вы можете настроить любой тип отчета по расписанию (ежедневный, еженедельный или ежемесячный) независимо друг от друга.

Отчеты, создаваемые по расписанию, содержат данные о работе всех узлов кластера. Выбор отдельных узлов недоступен.

► *Чтобы настроить параметры отчетов по расписанию:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите закладку **По расписанию**.
3. Нажмите на кнопку **Настроить расписание**.

   Откроется окно **Настроить расписание**.
4. Выберите одну из следующих закладок в зависимости от типа отчета, который вы хотите настроить:
   - **Ежедневно**. Отчет содержит данные с 00:00 до 23:59 предыдущего дня.
   - **Еженедельно**. Отчет содержит данные с 00:00 понедельника до 23:59 воскресенья предыдущей недели.
   - **Ежемесячно**. Отчет содержит данные с 00:00 первого числа до 23:59 последнего дня предыдущего месяца.
5. Переведите переключатель с названием типа отчета в положение **Включено**.
6. В блоке параметров **Расписание** задайте время регулярного создания отчетов.
7. Если вы хотите отправлять отчеты по электронной почте, в блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится новый блок параметров доставки отчета.
8. В поле **Адреса электронной почты** введите адреса, на которые вы хотите отправлять отчеты.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.
9. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправлять отчеты.
10. В раскрывающемся списке **Язык** выберите язык отчетов.
11. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка  справа от блока.
12. Нажмите на кнопку **Сохранить**.

Параметры отчетов по расписанию будут настроены. Как только первый отчет будет создан в указанное время, информация о нем (см. раздел "Просмотр информации об отчете" на стр. 187) отобразится в таблице отчетов. Вы сможете скачать отчет (см. раздел "Скачивание отчетов" на стр. 192) или отправить его по электронной почте (см. раздел "Отправка отчетов по электронной почте" на стр. 193).

Настройка отображения таблицы отчетов

По умолчанию в таблице отчетов отображаются все доступные графы. Если требуется, вы можете скрыть некоторые из них или изменить их очередность.

► *Чтобы настроить отображение таблицы отчетов:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите настроить таблицу отчетов, созданных разово по запросу пользователя.
   - **По расписанию**, если вы хотите настроить таблицу отчетов, созданных автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Нажмите на кнопку  в первой строке таблицы.

   Откроется окно **Настроить таблицу**.
4. Установите флажки напротив тех граф, которые должны отображаться в таблице.
5. Если вы хотите изменить расположение графы в таблице, в правой части строки с названием графы зажмите кнопку  и перетащите графу на нужное место.
6. Нажмите на кнопку **ОК**.

Отображение таблицы отчетов будет настроено.

Фильтрация и сортировка отчетов

Вы можете отсортировать все записи о созданных ранее отчетах по значению любой графы в таблице отчетов. С помощью значка  в заголовке графы можно изменять порядок сортировки по возрастанию или по убыванию.

Вы также можете отфильтровать отчеты по времени создания, временному интервалу содержащихся в них данных, а также по типу (только для отчетов по расписанию).

► *Чтобы отфильтровать отчеты:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите отфильтровать отчеты, созданные разово по запросу пользователя.

- **По расписанию**, если вы хотите отфильтровать отчеты, созданные автоматически по расписанию.

В рабочей области отобразится таблица созданных отчетов.

3. Нажмите на значок  .

Откроется окно **Фильтры**.

4. Нажмите на кнопку **Добавить фильтр**, чтобы добавить критерий фильтрации для поиска отчетов.
5. В появившихся полях задайте нужный критерий фильтрации. Для этого заполните поля фильтра согласно таблице ниже.

a. Выберите один из следующих критериев:	b. Выберите один из следующих логических операторов:	c. Укажите следующее значение:
Тип	• **равно**; • **не равно**.	Выберите тип отчета из раскрывающегося списка (применимо только для отчетов, созданных по расписанию): • **Ежедневный**; • **Еженедельный**; • **Ежемесячный**.
Время создания	• **после**; • **до**.	Временной диапазон создания отчета.
Начало периода	• **после**; • **до**.	Временной диапазон начала отчетного периода.
Окончание периода	• **после**; • **до**.	Временной диапазон окончания отчетного периода.

Вы можете указать несколько критериев фильтрации.

6. Нажмите на кнопку **Применить**.

Отчеты, удовлетворяющие параметрам поиска, отобразятся в таблице отчетов.

Просмотр информации об отчете

► Чтобы просмотреть информацию об отчете:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите просмотреть информацию об отчетах, созданных разово по запросу пользователя.
   - **По расписанию**, если вы хотите просмотреть информацию об отчетах, созданных автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, информацию о котором вы хотите просмотреть.

Откроется окно **Просмотреть информацию об отчете**.

В окне отображается следующая информация об отчете:

- **Время создания**. Время создания отчета.
- **Период**. Интервал времени, за который получена информация о работе программы, представленная в отчете.
- **Тип**. Тип отчета, созданного по расписанию:
  - **Ежедневный**.
  - **Ежемесячный**.
  - **Еженедельный**.

  Не отображается для отчетов, созданных по запросу пользователя.
- **Узлы**. IP-адреса и порты подключения тех узлов, информация о работе которых представлена в отчете (или **Все узлы**).
- **Параметры доставки**. Группа параметров доставки отчета по электронной почте, которая включает в себя список адресов, язык и формат отчета.
  - **При создании**. Параметры доставки, указанные во время создания отчета.
  - **При пересылке**. Параметры доставки, указанные для созданного ранее отчета при его пересылке на дополнительные адреса (см. раздел "Отправка отчетов по электронной почте" на стр. 193).

  В блоке **Параметры доставки** отображаются только уникальные группы параметров.
- **Результат**. Возможны следующие значения:
  - *Ошибка*.
  - *Ожидает*.
  - *Успешно*.

Содержание отчетов

Отчеты содержат следующую информацию о работе программы.

1. Блок **Общая информация**.
   - **Обнаружения**. Количество и объем обработанных сообщений, подсчитанных по каждому модулю программы в отдельности:
     - **Антивирус**.
     - **Проверка ссылок**.
     - **Защита KATA**.

       Отображается только при настроенной интеграции с KATA (см. раздел "Защита KATA" на стр. 228).

- **Анти-Фишинг**.
- **Анти-Спам**.
- **Проверка подлинности**.
- **Контентная фильтрация**.

- **Действия над сообщениями**. Количество и объем обработанных сообщений, подсчитанных по каждому типу выполненного программой действия:
  - **Не обнаружено**.
  - **Вылечено**.
  - **Удалены вложения**.
  - **Пропущено**.
  - **Не проверено**.
  - **Удалено**.
  - **Отклонено**.
  - **Помещено в Карантин**.
- **Узлы**. Количество и объем обработанных сообщений, подсчитанных по каждому узлу кластера, обрабатывающему почтовый трафик.

2. Блок **Типы объектов**.
   - **Антивирус**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Антивирус:
     - **Не обнаружено**.
     - **Обнаружено**.
     - **Вложения с макросами**.
     - **Непроверенные сообщения**.

       Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:
       - **Зашифровано**. Не удалось выполнить проверку, т.к. сообщение зашифровано.
       - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
       - **Параметры программы**. Отключена антивирусная проверка в общих параметрах защиты.
       - **Ограничения лицензирования**. Возникли проблемы с лицензией.
       - **Ошибка баз**. Отсутствуют антивирусные базы.
   - **Проверка ссылок**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки ссылок:
     - **Не обнаружено**.
     - **Обнаружено**.
     - **Непроверенные сообщения**.

Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

- **Ошибка проверки**. Возникла ошибка во время проверки ссылок.
- **Параметры программы**. Отключена проверка ссылок в общих параметрах защиты.
- **Ограничения лицензирования**. Возникли проблемы с лицензией.
- **Ошибка баз**. Отсутствуют базы программы.

- **Анти-Фишинг**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Анти-Фишинг:
  - **Не обнаружено**.
  - **Обнаружено**.
  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

    - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
    - **Параметры программы**. Отключена проверка модулем Анти-Фишинг в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы программы.
- **Анти-Спам**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки модулем Анти-Спам:
  - **Не обнаружено**.
  - **Обнаружено**.

    Обнаруженные объекты сгруппированы по следующим типам:

    - **Спам**.
    - **Предполагаемый спам**.
    - **Массовые рассылки**.
  - **На карантине**.
  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

    - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
    - **Параметры программы**. Отключена проверка модулем Анти-Спам в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы программы.
- **Проверка подлинности отправителей**. Количество сообщений за выбранный период, подсчитанных по каждому статусу проверки подлинности отправителя:
  - **Не обнаружено**.

- **Обнаружено**.
- **Непроверенные сообщения**.

  Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

  - **Параметры программы**. Отключена проверка подлинности отправителя в общих параметрах защиты.
  - **Ограничения лицензирования**. Возникли проблемы с лицензией.
  - **Ошибка баз**. Отсутствуют базы программы.

- **Контентная фильтрация**.
  - **Не обнаружено**.
  - **Обнаружено**.

    Обнаруженные объекты сгруппированы по следующим типам:

    - **Размер сообщения**. Превышен максимальный допустимый размер сообщения.
    - **Имя вложения**. Имя вложения соответствует критериям, заданным в правиле обработки сообщений.
    - **Тип вложения**. Формат вложения соответствует критериям, заданным в правиле обработки сообщений.

  - **Непроверенные сообщения**.

    Необработанные сообщения сгруппированы по следующим причинам невыполнения проверки:

    - **Ошибка проверки**. Возникла ошибка во время антивирусной проверки.
    - **Параметры программы**. Отключена контентная фильтрация в общих параметрах защиты.
    - **Ограничения лицензирования**. Возникли проблемы с лицензией.
    - **Ошибка баз**. Отсутствуют базы программы.

- **Примененные правила обработки сообщений**. Количество и объем сообщений, обработанных по каждому сработавшему правилу.

3. Блок **Статистика Антивируса**.
   - **Топ 10 полученных вредоносных объектов**. Имена самых частых вредоносных объектов в полученных сообщениях и количество срабатываний модуля Антивирус по каждому объекту.
   - **Топ 10 отправителей вредоносных объектов**. Адреса электронной почты самых частых отправителей вредоносных объектов, а также количество срабатываний модуля Антивирус по каждому отправителю.
   - **Топ 10 получателей вредоносных объектов**. Адреса электронной почты самых частых получателей вредоносных объектов, а также количество срабатываний модуля Антивирус по каждому получателю.
4. Блок **Статистика проверки ссылок**.
   - **Топ 10 источников вредоносных|рекламных|легальных ссылок**. IP-адреса серверов, с которых чаще всего отправлялись вредоносные/рекламные/легальные ссылки, а также количество срабатываний по каждому источнику.

- **Топ 10 получателей вредоносных|рекламных|легальных ссылок**. Адреса электронной почты самых частых получателей вредоносных/рекламных/легальных ссылок, а также количество срабатываний по каждому получателю.

5. Блок **Статистика Анти-Фишинга**.
   - **Топ 10 источников фишинга**. IP-адреса серверов, с которых чаще всего отправлялись фишинговые сообщения, а также количество срабатываний по каждому источнику.
   - **Топ 10 получателей фишинга**. Адреса электронной почты самых частых получателей фишинговых сообщений, а также количество срабатываний по каждому получателю.
6. Блок **Статистика Анти-Спама**.
   - **Топ 10 источников спама**. IP-адреса серверов, с которых чаще всего отправлялся спам или массовые рассылки, а также количество срабатываний по каждому источнику.
   - **Топ 10 получателей спама**. Адреса электронной почты самых частых получателей спама или массовых рассылок, а также количество срабатываний по каждому получателю.

Удаление отчетов

► Чтобы удалить отчет:

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите удалить отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите удалить отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите удалить.

   Откроется окно **Просмотреть информацию об отчете**.
4. В правом нижнем углу нажмите на кнопку **Удалить**.
5. В окне подтверждения нажмите на кнопку **ОК**.

Отчет будет удален.

Скачивание отчетов

► *Чтобы скачать отчет:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите скачать отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите скачать отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите скачать.

Откроется окно **Просмотреть информацию об отчете**.

4. В левом нижнем углу нажмите на кнопку **Скачать**.

   Откроется окно **Скачать отчет**.

5. В раскрывающемся списке **Язык** выберите язык отчета.
6. В раскрывающемся списке **Формат** выберите один из следующих форматов файла отчета:
   - **Html**.
   - **Pdf**.
7. В левом нижнем углу нажмите на кнопку **Скачать**.

Файл отчета будет сохранен на вашем компьютере в папке загрузки браузера.

Отправка отчетов по электронной почте

Вы можете указать адреса электронной почты, на которые требуется отправить отчет при его создании по требованию (см. раздел "Создание отчета по требованию" на стр. 184) или при настройке отчетов по расписанию (см. раздел "Настройка параметров отчетов по расписанию" на стр. 185).

Если требуется, вы можете переслать созданный ранее отчет на дополнительные адреса или отправить повторно на исходные адреса, указанные при создании отчета.

► *Чтобы отправить созданный ранее отчет по электронной почте:*

1. В окне веб-интерфейса программы выберите раздел **Отчеты**.
2. Выберите одну из следующих закладок:
   - **По требованию**, если вы хотите отправить отчет, созданный разово по запросу пользователя.
   - **По расписанию**, если вы хотите отправить отчет, созданный автоматически по расписанию.

   В рабочей области отобразится таблица созданных отчетов.
3. Выберите отчет, который вы хотите отправить.

   Откроется окно **Просмотреть информацию об отчете**.
4. В левом нижнем углу нажмите на кнопку **Доставить отчет**.

   Откроется окно **Доставить отчет**.
5. В блоке параметров **Параметры доставки** нажмите на кнопку **Добавить**.

   Отобразится новый блок параметров доставки отчета на дополнительные адреса.
6. В поле **Адреса электронной почты** введите адреса, на которые вы хотите переслать созданный ранее отчет.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.
7. В раскрывающемся списке **Формат** выберите формат файла, в котором требуется отправить отчет.
8. В раскрывающемся списке **Язык** выберите язык отчета.

9. Если требуется, вы можете добавить новый блок параметров с помощью кнопки **Добавить** или удалить ненужный с помощью значка  справа от блока.
10. Если вы хотите повторно отправить отчет на адреса, указанные при его создании, включите переключатель **Отправить повторно оригинальным получателям**.

    Переключатель не отображается, если при создании отчета по требованию или при настройке расписания автоматических отчетов вы не указали ни одного адреса в блоке **Параметры доставки**.

11. В левом нижнем углу нажмите на кнопку **Отправить**.

Отчет будет отправлен на указанные адреса. В нижней части рабочей области отобразится всплывающее окно с информацией о результате отправки.

kaspersky

Общие параметры защиты

Kaspersky Secure Mail Gateway обеспечивает защиту входящей и исходящей почты организации. Вы можете настроить следующие общие параметры защиты:

- Антивирусная защита.
- Проверка ссылок 203003.htm#anchor_LS.
- Защита сообщений от спама.
- Защита сообщений от фишинга.
- Контентная фильтрация сообщений.
- Проверка подлинности отправителей сообщений.

Общие параметры защиты применяются при проверке всех сообщений. Вы можете настроить действия над сообщениями по результатам проверки, а также дополнительные параметры с помощью правил обработки сообщений (см. раздел "Работа с правилами обработки сообщений" на стр. 98).

Антивирусная защита

Kaspersky Secure Mail Gateway выполняет антивирусную защиту сообщений: проверяет сообщения электронной почты на вирусы и другие программы, представляющие угрозу, а также лечит зараженные объекты с использованием информации текущей (последней) версии антивирусных баз.

Проверку сообщений на вирусы и другие программы, представляющие угрозу, выполняет модуль Антивирус. Модуль Антивирус проверяет тело сообщения и присоединенные к нему файлы любых форматов (вложения) с помощью антивирусных баз. Модуль Антивирус также позволяет обнаруживать и блокировать почтовые вложения, предназначенные для ограниченного числа получателей и представляющие собой компоненты целевых атак на уязвимости в программном обеспечении.

Вы можете настроить следующие параметры модуля Антивирус (см. стр. 204):

- использование эвристического анализа;
- максимальное время проверки сообщений;
- максимальный уровень проверки архивов;
- исключения из проверки некоторых легальных программ, которые могут быть использованы злоумышленниками.

По результатам проверки модуль Антивирус присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не заражено.
- *Заражено* – сообщение заражено, не может быть вылечено или лечение не проводилось.
- *Вылечено* – сообщение вылечено.
- *Зашифровано* – не удалось проверить объект из-за того, что он зашифрован.
- *Ошибка* – при проверке сообщения произошла ошибка.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки применения баз программы.
- *Угроза вторжения* – объект может быть использован злоумышленниками для вторжения в локальную сеть.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам программы.

- *Возможно зараженный* – объект содержит признаки вредоносного кода.

По умолчанию модуль Антивирус включен. Если требуется, вы можете отключить модуль Антивирус или отключить антивирусную проверку сообщений для любого правила (см. раздел "Настройка антивирусной защиты" на стр. 104).

Проверка ссылок

Kaspersky Secure Mail Gateway проверяет, являются ли ссылки в тексте сообщения вредоносными, рекламными или относящимися к легальным программам (на стр. 200), способным причинить вред компьютеру.

Вы можете настроить следующие параметры проверки ссылок (см. раздел "Настройка параметров проверки ссылок" на стр. 205):

- Максимальное время проверки сообщения.
- Исключения из проверки.

  Вы можете отключить обнаружение рекламных ссылок и ссылок, связанных с некоторыми легальными программами.

По результатам проверки ссылок программа присваивает сообщению один из следующих статусов:

- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз программы.
- *Не обнаружено* – сообщение не содержит ссылок, обнаружение которых включено согласно параметрам программы.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Обнаружено* – в сообщении содержатся вредоносные, рекламные или относящиеся к легальным программам ссылки.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам программы.

Защита сообщений от спама

Kaspersky Secure Mail Gateway фильтрует сообщения, проходящие через почтовый сервер, от нежелательной почты (спама).

Проверку сообщений на спам выполняет модуль Анти-Спам. Модуль Анти-Спам проверяет каждое сообщение на присутствие в нем признаков спама. Для этого модуль Анти-Спам, во-первых, проверяет атрибуты сообщения, такие, как: адреса отправителя и получателя, размер сообщения, заголовки (включая заголовки От и Кому). Во-вторых, модуль Анти-Спам анализирует содержание сообщения (включая заголовок Тема) и вложенных файлов.

Программа присваивает сообщению, в котором обнаружен спам или вероятный спам, определенный статус в соответствии со спам-рейтингом. *Спам-рейтинг сообщения* – это целое число от 0 до 100, которое складывается из баллов, начисленных сообщению программой за каждое срабатывание модуля Анти-Спам. При определении спам-рейтинга учитываются также ответы DNSBL- и SURBL-серверов, UDS-сервера, технологии SPF, а также результаты репутационной фильтрации сообщений.

При включении модуля Анти-Спам автоматически включается защита от BEC-атак. Это позволяет распознавать поддельные письма злоумышленников, направленные на компрометацию деловой переписки.

Вы можете настроить следующие параметры модуля Анти-Спам (см. стр. 206):

- Использование службы Moebius.

  Служба Moebius определяет разницу между текущей базой Анти-Спама, используемой в программе, и базой на сервере Moebius. После этого недостающие записи передаются на Управляющий узел по

протоколу HTTPS. Чтобы объем передаваемых данных не становился большим и служба Moebius работала стабильно, в программе должны регулярно обновляться базы Анти-Спама.

- Защиту от спуфинга Active Directory.

  Модуль Анти-Спам позволяет предотвращать спуфинговые атаки, в которых злоумышленники используют поддельное имя (Display Name) в заголовке сообщений From. При этом домен, с которого было отправлено сообщение, не совпадает с доменом организации. Вы можете указать в программе одну группу Active Directory численностью не более 10 000, к пользователям которой будет применяться защита от спуфинга.

- Проверку репутации IP-адресов и доменов.

  Эта опция позволяет проверять данные SMTP-сессии на основе записей о запрещенных IP-адресах и доменах в базах модуля Анти-Спам.

- Использование Анти-Спам карантина.

  Использование Анти-Спам карантина доступно только при участии в KSN.

  После помещения сообщения в Анти-Спам карантин программа обращается к серверам KSN для дальнейшей проверки сообщения. Использование облачной службы KSN повышает точность обнаружения признаков спама, так как базы KSN содержат более актуальную информацию, чем базы Анти-Спама, используемые в программе.

- Максимальное время проверки сообщений.
- Максимальное время хранения сообщения в Анти-Спам карантине
- Максимальное количество сообщений в Анти-Спам карантине.
- Максимальный размер Анти-Спам карантина.

По результатам проверки модуль Анти-Спам присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не содержит спам.
- *Спам* – программа однозначно расценивает сообщение как спам.
- *Предполагаемый спам* – возможно, сообщение является спамом.
- *В списке запрещенных адресов* – адрес электронной почты отправителя входит в глобальный или персональный список запрещенных адресов.
- *Массовая рассылка* – сообщение относится к массовой рассылке.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз программы.
- *Формальное сообщение* – программа расценивает сообщение как формальное автоматически сгенерированное уведомление (например, автоответы пользователей или уведомления о превышении размера почтового ящика).
- *Не проверено* – сообщение не было проверено согласно заданным параметрам программы.
- *Доверенный источник* – сообщение получено из доверенного источника (например, домен находится в списке доверенных или адрес добавлен в персональный список разрешенных адресов).

По результатам проверки программа добавляет в сообщение X-заголовок `X-MS-Exchange-Organization-SCL`, который содержит SCL-оценку.

Функциональность модуля Анти-Спам может быть изменена в результате редактирования файла настройки модуля Анти-Спам. В файле настройки можно изменить, например, статусы проверки сообщений на спам или уровень детализации записи данных сообщений электронной почты в журнале аудита и в журнале событий Kaspersky Secure Mail Gateway.
Доступ к файлу настройки модуля Анти-Спам может быть осуществлен из консоли управления Kaspersky Secure Mail Gateway в режиме Технической поддержки с правами учетной записи суперпользователя.

По умолчанию модуль Анти-Спам включен. Если требуется, вы можете отключить модуль Анти-Спам или отключить проверку сообщений на спам для любого правила (см. раздел "Настройка защиты от спама" на стр. 108).

Защита сообщений от фишинга

Kaspersky Secure Mail Gateway фильтрует сообщения, проходящие через почтовый сервер, от фишинга.

Проверку сообщений на наличие фишинга выполняет модуль Анти-Фишинг. Модуль Анти-Фишинг анализирует содержание сообщения (включая заголовок Тема) и вложенных файлов.

Вы можете настроить (см. раздел "Настройка параметров модуля Анти-Фишинг" на стр. 208)максимальное время проверки сообщений модулем Анти-Фишинг.

По результатам проверки модуль Анти-Фишинг присваивает сообщению один из следующих статусов:

- *Не обнаружено* – сообщение не содержит ссылок на фишинговые веб-адреса, изображений или текста, побуждающих пользователя предоставить конфиденциальные данные злоумышленникам, и не содержит ссылок на веб-ресурсы, содержащие вредоносные программы.
- *Фишинг* – программа обнаружила в сообщении изображение или текст, побуждающие пользователя предоставить конфиденциальные данные злоумышленникам.
- *Фишинговая ссылка* – программа обнаружила в сообщении ссылку на веб-ресурс, содержащий вредоносные программы.
- *Ошибка* – проверка сообщения завершена с ошибкой.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз программы.
- *Не проверено* – сообщение не было провереносогласно заданным параметрам программы.

По умолчанию модуль Анти-Фишинг включен. Если нужно, вы можете отключить модуль Анти-Фишинг или отключить проверку сообщений на фишинг для любого правила (см. раздел "Настройка защиты от фишинга" на стр. 110).

Контентная фильтрация сообщений

Kaspersky Secure Mail Gateway выполняет контентную фильтрацию сообщений, проходящих через почтовый сервер. Вы можете ограничить пересылку почтовым сервером сообщений с определенными параметрами.

Вы можете настроить следующие параметры контентной фильтрации (см. раздел "Настройка параметров контентной фильтрации" на стр. 208):

- максимальное время проверки сообщений;
- максимальный уровень проверки архивов.

В результате контентной фильтрации модуль управления проверкой сообщений Scan Logic присваивает сообщению один из следующих статусов контентной фильтрации:

- *Не обнаружено* – в сообщении не обнаружены нарушения ограничений, заданных в параметрах контентной фильтрации.
- *Запрещенное имя вложения* – сообщение содержит вложение с запрещенным именем.
- *Запрещенный формат вложения* – сообщение содержит вложение запрещенного формата.
- *Превышен допустимый размер* – превышен максимально разрешенный размер сообщения.
- *Ошибка баз* – не удалось проверить сообщение из-за ошибки баз программы.
- *Ошибка* – проверка сообщения завершилась с ошибкой.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам программы.

По умолчанию контентная фильтрация сообщений включена. Если нужно, вы можете отключить контентную фильтрацию в общих параметрах защиты или для любого правила (см. раздел "Настройка контентной фильтрации" на стр. 111).

Проверка подлинности отправителей сообщений

Проверка подлинности отправителей сообщений предназначена для дополнительной защиты почтовой инфраструктуры вашей организации от спама и фишинга.

Kaspersky Secure Mail Gateway использует следующие технологии проверки подлинности отправителей сообщений:

- SPF-проверку (Sender Policy Framework).
- DKIM-проверку (DomainKeys Identified Mail).
- DMARC-проверку (Domain-based Message Authentication, Reporting and Conformance).

SPF-проверка подлинности отправителей сообщений – сопоставление IP-адресов отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

Kaspersky Secure Mail Gateway получает списки возможных источников сообщений с DNS-сервера.

Включайте SPF-проверку, если Kaspersky Secure Mail Gateway принимает сообщения напрямую из интернета. Отключайте SPF-проверку, если Kaspersky Secure Mail Gateway принимает сообщения с внутреннего промежуточного сервера.

DKIM-проверка подлинности отправителей сообщений – проверка цифровой подписи к сообщениям.

К сообщениям добавляется цифровая подпись, связанная с именем домена организации. Kaspersky Secure Mail Gateway проверяет эту цифровую подпись.

DMARC-проверка подлинности отправителей сообщений – проверка, определяющая политику и действия над сообщениями по результатам SPF- и DKIM-проверок подлинности отправителей сообщений.

После того, как сообщение прошло SPF- и DKIM-проверки, выполняется проверка того, что домен, содержащий адрес отправителя в поле От заголовка сообщения электронной почты, соответствует идентификаторам SPF и DKIM.

kaspersky

Для выполнения SPF-, DKIM- и DMARC-проверок подлинности отправителей сообщений необходимо разрешить подключение Kaspersky Secure Mail Gateway к DNS-серверу. Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

По результатам проверки подлинности отправителей программа присваивает сообщению один из следующих статусов:

- *Не обнаружено* – в сообщении не обнаружены нарушения проверки подлинности.
- *Ошибка* – во время проверки подлинности произошла ошибка.
- *Аутентификация не пройдена* – не удалось выполнить проверку подлинности.
- *Не проверено* – сообщение не было проверено согласно заданным параметрам программы.
- *Обнаружено нарушение* – обнаружено нарушение хотя бы одной проверки подлинности.
- *Нарушение не обнаружено* – не обнаружено ни одного нарушения проверки подлинности.

По умолчанию все проверки подлинности отправителей включены. Если нужно, вы можете отключить любую проверку в общих параметрах защиты (см. раздел "Настройка параметров внешних служб" на стр. 209) или для любого правила (см. раздел "Проверка подлинности отправителей сообщений" на стр. 114).

Для того чтобы удаленный почтовый сервер мог проверить подлинность отправителя исходящих сообщений (если отправителем является Kaspersky Secure Mail Gateway), вам нужно предварительно добавить SPF- и DMARC-записи в параметры вашего DNS-сервера (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 210).

В этом разделе

Легальные программы – программы, разрешенные к установке и использованию на компьютерах пользователей и предназначенные для выполнения задач пользователя. Однако легальные программы некоторых типов при использовании злоумышленниками могут нанести вред компьютеру пользователя или компьютерной сети организации. Если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать некоторые функции таких программ для нарушения безопасности компьютера пользователя или компьютерной сети организации.

Среди таких программ – IRC-клиенты, программы автодозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Подобные программы описаны в таблице ниже.

Таблица 5. Легальные программы

Тип	Название	Описание
Client-IRC	Клиенты интернет-чатов	Пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.
Dialer	Программы автодозвона	Могут устанавливать телефонные соединения через модем в скрытом режиме.
Downloader	Программы-загрузчики	Могут загружать файлы с веб-страниц в скрытом режиме.
Monitor	Программы-мониторы	Позволяют наблюдать за активностью на том компьютере, на котором они установлены (видеть, какие приложения работают, и как они обмениваются данными с приложениями на других компьютерах).
PSWTool	Восстановители паролей	Позволяют просматривать и восстанавливать забытые пароли. С этой же целью их скрыто внедряют на компьютеры злоумышленники.
RemoteAdmin	Программы удаленного администрирования	Широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью злоумышленники скрыто внедряют их на компьютеры для наблюдения за компьютерами и управления ими. Легальные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями, которые позволяют им самостоятельно проникать в систему и устанавливать себя; легальные программы этих функций не имеют.
Server-FTP	FTP-серверы	Выполняют функции FTP-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу FTP.
Server-Proxy	Прокси-серверы	Выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
Server-Telnet	Telnet-серверы	Выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу Telnet.
Server-Web	Веб-серверы	Выполняют функции веб-сервера. Злоумышленники внедряют их на компьютеры, чтобы открыть к ним удаленный доступ по протоколу HTTP.
RiskTool	Инструменты для работы на виртуальной машине	Дают пользователю дополнительные возможности при работе на компьютере (позволяют скрывать файлы или окна активных приложений, закрывать активные процессы).

Тип	Название	Описание
NetTool	Сетевые инструменты	Дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).
Client-P2P	Клиенты пиринговых сетей	Позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.
Client-SMTP	SMTP-клиенты	Отправляют сообщения электронной почты в скрытом режиме. Злоумышленники внедряют их на компьютеры, чтобы от их имени рассылать спам.
WebToolbar	Веб-панели инструментов	Добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.
FraudTool	Псевдопрограммы	Выдают себя за другие программы. Например, существуют псевдоантивирусы, которые выводят на экран сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

Настройка параметров модуля Антивирус

► *Чтобы настроить параметры модуля Антивирус, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Антивирус**.
3. Включите или отключите модуль Антивирус с помощью переключателя **Использовать Антивирус**.

   По умолчанию модуль Антивирус включен.
4. Если на предыдущем шаге вы включили модуль Антивирус, настройте следующие параметры антивирусной проверки:
   a. Если вы хотите использовать технологию обнаружения угроз, не определяемых с помощью антивирусных баз, включите функцию эвристического анализа с помощью переключателя **Использовать эвристический анализ**.

      По умолчанию эвристический анализ включен.
   b. Если вы включили использование эвристического анализа, в раскрывающемся списке **Уровень эвристического анализа** выберите один из следующих уровней:
      - **Поверхностный**.
      - **Средний**.
      - **Глубокий**.

      По умолчанию выбран уровень **Средний**.
   c. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время антивирусной проверки сообщений в секундах.

      Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 180.

Если антивирусная проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

- Прерывает проверку сообщения.
- Выполняет действие над сообщением, которое вы настроили.
- Присваивает сообщению статус *Ошибка.*
- Добавляет запись в журнал событий /var/log/ksmg-messages.

d. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности сообщений, проверяемых модулем Антивирус.

Возможные значения – целые числа от 1 до 20000. Значение по умолчанию – 32.

5. Если требуется, настройте исключения из антивирусной проверки. Для этого в блоке параметров **Исключения из проверки** включите или отключите антивирусную проверку легальных программ[2], которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, с помощью переключателя **Некоторые легальные программы**.

> По умолчанию сообщения, в которых обнаружены легальные программы, исключаются из проверки. При отключении этого параметра к таким сообщениям будет применяться действие, указанное в правилах для зараженных объектов.

6. Нажмите на кнопку **Сохранить**.

Параметры модуля Антивирус будут настроены.

Настройка параметров проверки ссылок

Вы можете включить проверку ссылок, чтобы отслеживать ссылки, ведущие на вредоносные веб-ресурсы, а также рекламные ссылки и ссылки, относящиеся к легальному ПО, которое при использовании злоумышленниками может нанести вред компьютерной сети вашей организации.

► *Чтобы настроить параметры проверки ссылок:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Проверка ссылок**.
3. Включите или отключите проверку ссылок с помощью переключателя **Проверять ссылки**.

   По умолчанию проверка ссылок включена.
4. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений в секундах.

   Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

   Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

[2] К легальным программам, которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, относятся, например, коммерческие утилиты удаленного администрирования, программы-клиенты IRC, программы дозвона, программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями.

- Прерывает проверку сообщения.
- Выполняет действие над сообщением, которое вы настроили.
- Присваивает сообщению статус *Ошибка*.
- Добавляет запись в журнал событий /var/log/ksmg-messages.

5. Если требуется, настройте исключения из проверки. Для этого в блоке параметров **Исключения из проверки** выполните следующие действия:
   - Включите или отключите проверку рекламных программ с помощью переключателя **Рекламные ссылки**.

     По умолчанию этот параметр включен, то есть проверка рекламных программ не выполняется.
   - Включите или отключите проверку ссылок на некоторые легальные программы, которые при использовании злоумышленниками могут нанести вред компьютерной сети вашей организации, с помощью переключателя **Ссылки, связанные с некоторыми легальными программами**.

     По умолчанию этот параметр включен, то есть проверка ссылок на некоторые легальные программы не выполняется.
6. Нажмите на кнопку **Сохранить**.

Параметры проверки ссылок будут настроены.

Настройка параметров модуля Анти-Спам

Модуль Анти-Спам проверяет только первые 50 МБ сообщения. При превышении этого размера сообщение не будет проверено полностью, а статус будет присвоен на основе проверки первых 50 МБ.

► *Чтобы настроить параметры модуля Анти-Спам, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Спам**.
3. Включите или отключите модуль Анти-Спам с помощью переключателя **Использовать Анти-Спам**.

   По умолчанию модуль Анти-Спам включен.
4. Если на предыдущем шаге вы включили модуль Анти-Спам, настройте следующие параметры:
   a. Включите или отключите службу Moebius с помощью переключателя **Использовать службу Moebius**.

      По умолчанию служба Moebius включена.
   b. Включите или отключите защиту от спуфинговых атак с помощью переключателя **Защита от спуфинга Active Directory**.

      По умолчанию защита от спуфинговых атак отключена.
   c. Если на предыдущем шаге вы включили защиту от спуфинговых атак, в поле **Группа LDAP: distinguishedName** укажите группу Active Directory, к пользователям которой будет применяться защита.

Вы можете добавить только одну группу. Количество записей в группе, содержащих адрес электронной почты, не должно превышать 10 000. При превышении этого количества защита спуфинговых атак будет применена к случайным 10 000 пользователей из этой группы.

d. Включите или отключите проверку репутации IP-адресов и доменов, с которых были отправлены сообщения, по базам модуля Анти-Спам с помощью переключателя **Репутация IP-адресов и доменов**.

   По умолчанию проверка репутации IP-адресов и доменов включена.

e. Включите или отключите использование Анти-Спам карантина с помощью переключателя **Использовать Анти-Спам карантин**.

   Если использование Анти-Спам карантина включено, сообщения электронной почты, для которых результат проверки модулем Анти-Спам не окончателен, временно помещаются в Анти-Спам карантин.

   Изменение значений для параметров Анти-Спам карантина, установленных по умолчанию, может привести к снижению уровня обнаружения спама.

f. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений на спам в секундах.

   Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

   Если проверка сообщения на спам не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

   - Прерывает проверку сообщения (действие **Пропустить**).
   - Присваивает сообщению статус *Ошибка.*
   - Доставляет сообщение получателю.
   - Добавляет запись в журнал событий /var/log/ksmg-messages.

5. В поле **Максимальное время хранения сообщения (сек.)** укажите время нахождения сообщения в Анти-Спам карантине, по истечении которого сообщение будет доставлено получателю.

   Возможные значения – целые числа от 1 до 86400. Значение по умолчанию – 3000.

6. В поле **Максимальное количество сообщений** укажите количество сообщений, при превышении которого сообщения не будут помещаться в карантин.

   Укажите 0, если ограничения не требуются.

   Возможные значения – целые числа от 0 до 9007199254740993. Значение по умолчанию – 0.

7. В поле **Максимальный размер карантина (МБ)** укажите размер Анти-Спам карантина, при превышении которого сообщения не будут помещаться в карантин.

   Возможные значения – целые числа от 0 до 8192. Значение по умолчанию – 1024.

8. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Спам будут настроены.

kaspersky

Настройка параметров модуля Анти-Фишинг

► *Чтобы настроить параметры модуля Анти-Фишинг, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Анти-Фишинг**.
3. Включите или отключите модуль Анти-Фишинг с помощью переключателя **Использовать Анти-Фишинг**.

   По умолчанию модуль Анти-Фишинг включен.
4. Если на предыдущем шаге вы включили модуль Анти-Фишинг, в поле **Максимальная длительность проверки (сек.)** укажите максимальное время проверки сообщений на фишинг в секундах.

   Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

   Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

   - Прерывает проверку сообщения.
   - Выполняет действие над сообщением, которое вы настроили.
   - Присваивает сообщению статус *Ошибка.*
   - Добавляет запись в журнал событий /var/log/ksmg-messages.
5. Нажмите на кнопку **Сохранить**.

Параметры модуля Анти-Фишинг будут настроены.

Настройка параметров контентной фильтрации

► *Чтобы настроить параметры контентной фильтрации, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Контентная фильтрация**.
3. Включите или отключите контентную фильтрацию с помощью переключателя **Использовать Контентную фильтрацию**.

   По умолчанию контентная фильтрация включена.
4. Если на предыдущем шаге вы включили контентную фильтрацию, настройте следующие параметры:

   a. В поле **Максимальная длительность проверки (сек.)** укажите максимальное время контентной проверки сообщений в секундах.

      Возможные значения – целые числа от 1 до 600. Значение по умолчанию – 30.

      Если проверка сообщения не успевает завершиться за указанное вами время, Kaspersky Secure Mail Gateway выполняет следующие действия:

      - Прерывает проверку сообщения (действие **Пропустить**).
      - Присваивает сообщению статус *Ошибка*.

- Доставляет сообщение получателю.
- Добавляет запись в журнал событий /var/log/ksmg-messages.

b. В поле **Максимальная глубина проверки архивов** укажите максимальный уровень вложенности сообщений, до которого выполняется контентная фильтрация.

Возможные значения – целые числа от 1 до 20000. Значение по умолчанию – 32.

> Если задать для этого поля значение, отличное от 0, то программа будет проверять архивы только до заданной глубины, даже если их уровень вложенности превышает заданное значение. Если в архиве до заданной глубины не было найдено нарушений ограничений, заданных в параметрах контентной фильтрации, программа будет отображать результат проверки *Не обнаружено*.

5. Нажмите на кнопку **Сохранить**.

Параметры контентной фильтрации будут настроены.

Настройка параметров внешних служб

► *Чтобы настроить параметры внешних служб, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Защита**.
2. Выберите закладку **Внешние службы**.
3. Разрешите или запретите подключение к DNS-серверу с помощью переключателя **Разрешить подключение к DNS-серверу**.

   По умолчанию подключение разрешено.

   > Если подключение к DNS-серверу запрещено, SPF-, DKIM- и DMARC-проверки подлинности отправителей сообщений будут отключены.

4. В поле **Время ожидания DNS-сервера (с)** укажите максимальное время ожидания ответа DNS-сервера в секундах.

   Значение по умолчанию – 10 сек. По истечении этого времени DNS-сервер будет считаться недоступным, и сообщение будет обработано программой без проверки подлинности отправителей.
5. В поле **Время ожидания сервера KSN (с)** укажите максимальное время ожидания ответа сервера KSN в секундах.

   Значение по умолчанию – 10 сек. По истечении этого времени сервер KSN будет считаться недоступным, и сообщение будет обработано программой без проверки с помощью репутационной базы KSN.

   > Опция используется, только если вы согласились участвовать в программе Kaspersky Security Network или Kaspersky Private Security Network.

6. Включите или отключите SPF-проверку подлинности отправителей с помощью переключателя **Использовать SPF-проверку**.

Если вы включили SPF-проверку подлинности отправителей, программа будет сопоставлять IP-адреса отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

> Перед включением SPF-проверки требуется выполнить предварительную настройку (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 210) на DNS-сервере.

По умолчанию проверка включена.

7. Включите или отключите DKIM-проверку подлинности отправителей с помощью переключателя **Использовать DKIM-проверку**.

   Если вы включили DKIM-проверку подлинности отправителей, программа будет проверять цифровую подпись к сообщениям.

   По умолчанию проверка включена.

8. Включите или отключите DMARC-проверку подлинности отправителей с помощью переключателя **Использовать DMARC-проверку**.

   Если вы включили DMARC-проверку подлинности отправителей, программа будет проверять, соответствует ли идентификаторам SPF и DKIM домен, содержащий адрес отправителя в поле "От" заголовка сообщения электронной почты.

   > Перед включением DMARC-проверки требуется выполнить предварительную настройку (см. раздел "Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений" на стр. 210) на DNS-сервере.

   По умолчанию проверка включена.

9. Нажмите на кнопку **Сохранить**.

Параметры внешних служб будут настроены.

Подготовка к настройке SPF- и DMARC-проверок подлинности отправителя сообщений для исходящих сообщений

Для того чтобы удаленный почтовый сервер мог проверить подлинность отправителя сообщений, если отправителем сообщений является Kaspersky Secure Mail Gateway (подлинность отправителя исходящих сообщений), вам нужно добавить SPF- и DMARC-записи в параметры вашего DNS-сервера.

► *Чтобы добавить SPF- и DMARC-записи в параметры вашего DNS-сервера, выполните следующие действия:*

1. Авторизуйтесь на вашем DNS-сервере под учетной записью администратора.
2. Найдите страницу, содержащую информацию об обновлении DNS-записей того домена, для адресов которого вы хотите настроить проверку подлинности отправителя исходящих сообщений.

   Например, страница может носить название "Управление DNS", "Управление сервером имен" или "Дополнительные настройки".

3. Найдите записи формата TXT того домена, для адресов которого вы хотите настроить проверку подлинности отправителя исходящих сообщений.
4. В списке записей формата TXT добавьте SPF-запись для определенного домена следующего содержания:

   ```
   <имя домена, для адресов которого вы хотите настроить SPF-проверку подлинности отправителя исходящих сообщений> IN TXT "v=<версия SPF> +all>"
   ```

   Например, вы можете добавить строку:

   ```
   example.com IN TXT "v=spf1 +all"
   ```

   > Подробнее о назначении параметров SPF-записи см. в документе RFC 7208.

5. В списке записей формата TXT добавьте DMARC-запись для определенного домена следующего содержания:

   ```
   _dmarc.<имя домена, для адресов которого вы хотите настроить DMARC-проверку подлинности отправителя исходящих сообщений>. IN TXT "v=<версия DMARC>; p=<действие, которое удаленный почтовый сервер будет производить над всеми сообщениями электронной почты, не удовлетворяющими требованиям DMARC>;"
   ```

   Например, вы можете добавить строку:

   ```
   _dmarc.example.com. IN TXT "v=DMARC1; p=quarantine;"
   ```

   > Подробнее о назначении параметров DMARC-записи см. в документации DMARC.

6. Сохраните изменения.

> Синтаксис примеров SPF- и DMARC-записей приведен для добавления в параметры DNS-сервера BIND. Синтаксис SPF- и DMARC-записей, добавляемых в параметры других DNS-серверов, может незначительно отличаться от приведенных примеров.

kaspersky

Настройка даты и времени

Вы можете настроить время сервера, используемое в параметрах программы. Обновления баз и правила обработки сообщений, для которых задано расписание, будут применяться согласно установленному времени.

► *Чтобы настроить время сервера, выполните следующие действия:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Общие** → **Дата и время**.
2. В блоке параметров **Часовой пояс** выполните следующие действия:
   a. В раскрывающемся списке **Страна** выберите страну, к которой относится нужный часовой пояс.
   b. В раскрывающемся списке **Часовой пояс** выберите часовой пояс.
3. В блоке параметров **Синхронизация времени** включите или отключите синхронизацию с NTP-сервером с помощью переключателя **Синхронизировать с NTP-сервером**.

   Если вы развернули ISO-образ программы на виртуальной машине VMware, то при включении синхронизации с NTP-сервером синхронизация времени с гипервизором будет отключена автоматически. Если вы используете гипервизор Hyper-V синхронизацию времени можно включить или отключить в свойствах виртуальной машины в разделе **Settings** → **Integration Service** с помощью флажка **Time Synchronization**.

4. Если вы включили синхронизацию с NTP-сервером, в поле **NTP-сервер** введите полное доменное имя (FQDN) или IP-адрес NTP-сервера в формате IPv4 или IPv6 и нажмите клавишу **ENTER**.

   Вы можете вводить адреса по одному или добавить сразу весь список серверов, разделенных точкой с запятой.

5. Нажмите на кнопку **Сохранить**.

Дата и время будут настроены. Внесенные изменения будут сохранены на Управляющем узле и распространены на все узлы кластера. Состояние синхронизации времени будет отображаться в информации о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130).

Настройка параметров соединения с прокси-сервером

Заданные параметры прокси-сервера будут использованы для обновления баз, активации программы, а также работы служб KSN/KPSN и службы Moebius.

► *Чтобы настроить параметры соединения с прокси-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Соединение с прокси-сервером**.
2. Включите или отключите использование прокси-сервера с помощью переключателя **Использовать прокси-сервер**.
3. Если на предыдущем шаге вы включили использование прокси-сервера, то в полях **Адрес прокси-сервера** введите адрес и номер порта прокси-сервера.

   По умолчанию используется порт 8080.
4. Установите флажок **Не использовать прокси-сервер для локальных и частных адресов**, если вы не хотите использовать прокси-сервер для внутренних и частных адресов электронной почты.
5. В полях **Имя пользователя (необязательно)** и **Пароль (необязательно)** введите имя пользователя и пароль, если вы хотите использовать аутентификацию при подключении к прокси-серверу.
6. Нажмите на кнопку **Сохранить**.

Параметры соединения с прокси-сервером будут настроены.

kaspersky

Загрузка пакетов обновлений

"Лаборатория Касперского" может выпускать пакеты обновлений Kaspersky Secure Mail Gateway. Например, могут выпускаться срочные пакеты обновлений, устраняющие уязвимости и ошибки, плановые обновления, добавляющие новые или улучшающие существующие функции Kaspersky Secure Mail Gateway, пакеты дополнительных локализаций Kaspersky Secure Mail Gateway.

После выпуска обновлений Kaspersky Secure Mail Gateway вы можете установить их через веб-интерфейс Kaspersky Secure Mail Gateway.

Перед установкой обновлений через веб-интерфейс Kaspersky Secure Mail Gateway вам нужно загрузить пакет обновления или пакет локализации формата TGZ и инструкцию по установке данного обновления с сайта интернет-магазина на ваш компьютер.

Службы Kaspersky Secure Mail Gateway могут быть приостановлены на время установки обновления. Процесс обновления может занять несколько минут. После запуска обновления Kaspersky Secure Mail Gateway не следует прерывать процесс обновления или выключать виртуальную машину. После установки обновлений может потребоваться перезапуск Kaspersky Secure Mail Gateway.

Централизованная установка пакетов обновлений на все узлы кластера не предусмотрена. Требуется выполнить шаги по обновлению отдельно на каждом узле кластера.

Функциональность доступна только при наличии права **Изменять параметры**.

Перед обновлением Kaspersky Secure Mail Gateway настоятельно рекомендуется сделать копию вашей виртуальной машины Kaspersky Secure Mail Gateway (моментальный снимок виртуальной машины в гипервизоре) для того, чтобы у вас была возможность вернуться к предыдущей версии Kaspersky Secure Mail Gateway, если установка новой версии Kaspersky Secure Mail Gateway завершится неудачно.

► *Чтобы загрузить пакет обновлений и начать его установку:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Установить обновление**.
2. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
3. Выберите файл обновления, который вы хотите загрузить, и нажмите на кнопку **Open**.

   Имя загруженного файла отобразится сверху над областью загрузки.
4. Нажмите на кнопку **Обновить**.
5. Следуйте шагам мастера обновления.

   Шаги мастера обновления могут различаться в зависимости от типа загружаемого обновления.

Более подробное описание установки каждого обновления приведено в руководстве по установке этого обновления.

kaspersky

Обновление баз Kaspersky Secure Mail Gateway

Базы модулей Антивирус, Анти-Спам и Анти-Фишинг (далее также "базы") представляют собой файлы с записями, которые позволяют обнаруживать в проверяемых объектах вредоносный код. Эти записи содержат информацию о контрольных участках вредоносного кода и алгоритмы лечения объектов, в которых содержатся угрозы.

Вирусные аналитики "Лаборатории Касперского" ежедневно обнаруживают множество новых угроз, создают для них идентифицирующие записи и включают их в *пакет обновлений баз* (далее также "пакет обновлений"). Пакет обновлений представляет собой один или несколько файлов с записями, идентифицирующими угрозы, которые были выявлены за время, прошедшее с момента выпуска предыдущего пакета обновлений. Чтобы свести риск заражения защищаемого почтового сервера к минимуму, рекомендуется регулярно получать пакеты обновлений.

В течение срока действия лицензии вы можете получать пакеты обновлений автоматически по расписанию (см. раздел "Настройка расписания и параметров обновления баз" на стр. 217) или устанавливать пакеты обновлений вручную (см. раздел "Запуск обновления баз вручную" на стр. 218), загружая их с веб-сайта "Лаборатории Касперского".

Об источниках обновлений

Во время установки Kaspersky Secure Mail Gateway получает текущие базы с одного из серверов обновлений "Лаборатории Касперского". После установки доступно несколько источников обновлений.

Основным источником обновлений служат серверы обновлений "Лаборатории Касперского". Это специальные интернет-сайты, на которые выкладываются обновления баз и программных модулей для всех программ "Лаборатории Касперского". Если для доступа в интернет вы используете прокси-сервер, вам нужно настроить параметры подключения к прокси-серверу (см. раздел "Настройка параметров соединения с прокси-сервером" на стр. 213).

Чтобы уменьшить интернет-трафик, вы можете настроить обновление баз из *пользовательского источника обновлений.* Пользовательским источником обновлений могут служить указанные вами HTTP- или FTP-серверы, а также локальные папки на вашем компьютере.

Мониторинг состояния баз

Kaspersky Secure Mail Gateway периодически автоматически проверяет наличие новых пакетов обновлений на серверах обновлений "Лаборатории Касперского". Статусы баз программы в зависимости от времени последнего обновления описаны в таблице ниже.

Таблица 6. Статусы баз программы

Модуль проверки	Актуальны	Устарели	Сильно устарели
Антивирус	менее 24 часов	от 24 часов до 7 суток	более 7 суток
Анти-Спам	менее 5 часов	от 5 до 24 часов	более 24 часов
Анти-Фишинг	менее 48 часов	от 48 до 72 часов	более 72 часов

Актуальное состояние баз программы (см. раздел "Мониторинг состояния баз программы" на стр. 219) отображается на информационной панели **Лицензирование**, а также в таблице с информацией о базах на каждом узле кластера в разделе **Параметры → Внешние службы → Обновление баз → Статус обновления**.

kaspersky

В этом разделе

Настройка расписания и параметров обновления баз

► *Чтобы настроить расписание и параметры обновления баз, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. Выберите закладку **Параметры обновления**.
3. В раскрывающемся списке **Источник** выберите один из следующих источников обновлений:
   - **Серверы "Лаборатории Касперского" (безопасное соединение)**.
   - **Серверы "Лаборатории Касперского" (небезопасное соединение)**.
   - **Пользовательский**.

   По умолчанию установлено значение **Серверы "Лаборатории Касперского" (безопасное соединение)**.
4. Если на предыдущем шаге вы выбрали **Пользовательский**, в поле **Пользовательский источник** укажите адрес пользовательского источника, из которого вы хотите получать пакеты обновлений. Вы можете указать следующие источники:
   - URL-адрес сервера обновления.

     Для серверов, использующих протокол HTTPS, обновление будет выполняться, только если указан сервер "Лаборатории Касперского".

   - Локальную папку.

     Требуется указать полный путь к папке обновления, расположенной на всех узлах кластера. Если папка по указанному пути отсутствует на Управляющем узле, то администратору отображается уведомление. Если указанной папки нет на Подчиненном узле, то для этого узла обновление баз будет выполняться со старыми параметрами.

   - Сетевую папку, то есть папку на удаленном компьютере, смонтированную по протоколам SMB или NFS.

   Вы также можете установить флажок **При недоступности использовать серверы "Лаборатории Касперского"**, если вы хотите получать пакеты обновлений с серверов обновлений "Лаборатории Касперского", когда ваш источник обновлений недоступен. По умолчанию флажок снят.
5. В раскрывающемся списке **Расписание** выберите один из вариантов и выполните следующие действия для настройки расписания:
   - **Вручную**.
   - **Один раз**. В появившемся поле укажите дату и время запуска обновления баз.

- **Дня(ей)**. В появившемся поле укажите время ежедневного запуска обновления баз.
- **Еженедельно**. В появившихся полях укажите день недели и время запуска обновления баз.

  Например, если установлены значения **Пн** и **15:00**, обновление баз запускается каждый понедельник в 15 часов.
- **Ежемесячно**. В появившихся полях укажите день месяца и время запуска обновления баз.

  Например, если установлены значения **20** и **15:00**, обновление баз запускается каждый месяц двадцатого числа в 15 часов.
- **Запускать каждые**. В появившихся полях укажите периодичность запуска обновления баз в минутах, часах или днях.

  Например, если для периодичности установлено значение **30** и выбрана периодичность **Минуту(ы)**, то обновление баз запускается каждые полчаса.

Первое обновление баз запустится сразу после сохранения внесенных изменений.

По умолчанию обновление баз запускается каждые 15 минут.

6. В поле **Максимальная длительность (мин)** укажите максимальное время выполнения обновления баз в минутах, по истечении которого обновление баз должно быть остановлено.

   Если задача обновления баз не завершена за указанное время, она запустится в следующий раз, указанный в расписании.

   По умолчанию установлено значение 180.
7. Переведите переключатель **Запускать пропущенные задачи** в положение **Включено**, если вы хотите запускать пропущенные задачи обновления баз при последующем запуске программы.

   Обновление могло не выполняться в заданное расписанием время, например, если компьютер был выключен или если программа не была запущена.

   > Если запуск пропущенных задач выключен, то пропущенные задачи обновления баз не будут запущены при последующем запуске программы. Следующий запуск обновления баз будет выполнен согласно расписанию.

   По умолчанию запуск пропущенных задач включен.
8. Нажмите на кнопку **Сохранить**.

Расписание и параметры обновления баз будут настроены.

Запуск обновления баз вручную

> Функциональность доступна только при наличии права **Изменять параметры**.

► *Чтобы запустить обновление баз вручную, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Обновление баз**.
2. Выберите закладку **Статус обновления**.

3. Нажмите на кнопку **Обновить базы**.

Обновление баз будет запущено. В нижней части окна отобразится сообщение о статусе задачи обновления.

Мониторинг состояния баз программы

Чтобы отслеживать проблемы, связанные с обновлением баз программы, вы можете просматривать сводную информацию о состоянии баз на всех узлах кластера на информационной панели **Обновление баз** в разделе **Узлы**.

Возможны следующие статусы:

- *Без ошибок* – все базы программы обновлены, в процессе обновления не возникло ошибок.
- *Базы устарели* – обработка трафика не остановлена, и возникло хотя бы одно из следующих событий:
  - базы Антивируса не обновлялись от 24 часов до 7 суток;
  - базы Анти-Спама не обновлялись от 5 до 24 часов;
  - базы Анти-Фишинга не обновлялись от 48 до 72 часов.
- *Базы сильно устарели* – обработка трафика не остановлена, и возникло хотя бы одно из следующих событий:
  - базы Антивируса не обновлялись более 7 суток;
  - базы Анти-Спама не обновлялись более 24 часов;
  - базы Анти-Фишинга не обновлялись более 72 часов.
- *Ошибки* – возникло одно из следующих событий:
  - отсутствуют базы для одного или более модулей проверки;
  - на одном или нескольких узлах кластера остановлена обработка трафика;
  - один или несколько узлов кластера недоступен, нет возможности получить информацию о состоянии баз программы.

Под чертой в поле *Ошибки последнего обновления* отображается количество узлов кластера, на которых последняя задача обновления завершилась с ошибкой.

► *Чтобы просмотреть детальную информацию о состоянии баз программы на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Обновление баз** перейдите в раздел **Параметры** → **Внешние службы** → **Обновление баз** → **Статус обновления**.

В рабочей области отображается таблица узлов кластера с информацией о базах программы по каждому модулю проверки:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Антивирус** – состояние антивирусных баз.
- **Анти-Фишинг** – состояние баз модуля Анти-Фишинг.

- **Анти-Спам** – состояние баз модуля Анти-Спам.
- **Статус обновления** – статус последней задачи обновления:
  - если задача завершилась успешно, отображается время завершения этой задачи;
  - если задача завершилась с ошибкой, отображается время запуска текущей задачи и время последнего успешного обновления баз (при наличии).
  - если задача еще ни разу не была запущена после установки программы или если узел кластера недоступен, отображается прочерк.
  - если задача находится в процессе, отображается процент ее выполнения.

Таблица отображается при наличии у пользователя прав **Просматривать информацию об узлах** и/или **Создавать/изменять/удалять узлы**, а также **Просматривать параметры** и/или **Изменять параметры**.

Вы также можете просмотреть сведения о состоянии баз программы в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130).

kaspersky

Экспорт и импорт параметров

Функциональность доступна при наличии у пользователя права **Изменять параметры**.

Экспорт и импорт параметров Kaspersky Secure Mail Gateway может быть использован для следующих целей:

- Резервное копирование параметров программы.

  Если вам потребуется развернуть программу на новом сервере, вы сможете импортировать ранее экспортированные параметры правил, а также персональные списки разрешенных и запрещенных адресов. Это позволит сократить время на конфигурацию нового узла.

- Миграция программы на новую версию (см. раздел "Миграция параметров из более старой версии" на стр. 222).

  Перед обновлением программы вы можете экспортировать параметры из старой версии и импортировать их в новую версию.

  Миграция с более новой на более старую версию не поддерживается.

При экспорте параметров (см. раздел "Экспорт параметров" на стр. 221) создается конфигурационный файл, содержащий версию программы и значения параметров. Созданный конфигурационный файл сохраняется локально на Управляющем узле.

При импорте конфигурационного файла (см. раздел "Импорт параметров" на стр. 222) вы можете выбрать, какие параметры должны быть применены:

- правила обработки сообщений (включая предустановленные правила Allowlist и Denylist);
- персональные списки разрешенных и запрещенных адресов.

Значения остальных параметров не будут изменены после завершения импорта.

В этом разделе

Экспорт параметров

► *Чтобы экспортировать параметры:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Экспорт**.

3. Нажмите на кнопку **Экспортировать**.

   В таблице ниже отобразится текущее состояние операции экспорта. После успешного завершения операции отобразится строка с датой и временем экспорта.

4. Нажмите на значок  в нужной строке.

Конфигурационный файл с экспортированными параметрами будет сохранен в папке загрузки браузера.

Импорт параметров

► *Чтобы импортировать параметры:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Импорт**.
3. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.

4. Выберите файл с ранее экспортированными параметрами.

   Под областью загрузки отобразится блок параметров **Импортировать параметры**.

5. Установите флажки напротив тех параметров, которые вы хотите импортировать.
6. Нажмите на кнопку **Импортировать**.

Отобразится сообщение о результате выполнения операции импорта.

Миграция параметров из более старой версии

Доступна миграция параметров только из версии Kaspersky Secure Mail Gateway 1.1 Maintenance Release 3 (далее также "версия 1.1 MR3"). Миграция из более ранних версий программы не поддерживается.

Сценарий миграции параметров включает в себя следующие этапы.

a. **Экспорт параметров из версии 1.1 MR 3** https://support.kaspersky.com/KSMG/1.1.3/ru-RU/144241.htm

   В эскпортированном конфигурационном файле сохраняются параметры правил обработки сообщений (включая предустановленные правила Allowlist и Denylist), а также персональные списки разрешенных и запрещенных адресов.

b. **Импорт параметров в версию 2.0 (см. раздел "Импорт параметров" на стр. 222)**

   В результате импорта для выбранных параметров будут установлены значения из конфигурационного файла.

Импорт правил обработки сообщений осуществляется по следующему алгоритму:

- Для параметра уведомлений **Уведомить получателей из общего списка** в версии 2.0 устанавливается значение параметра **Уведомлять администратора** версии 1.1 MR3.
- Удаляются параметры версии 1.1 MR3, отсутствующие в версии 2.0:
  - параметры модуля Антивирус (ограничение по размеру сообщений, исключения из проверки вложений по типам файлов);
  - параметры модуля Анти-Спам (обработка сообщений на основе списка DNSBL, использование пользовательских списков DNSBL и SURBL, увеличение спам-рейтинга для сообщений, написанных на выбранных языках, проверка вложений в формате RTF, ограничение по размеру сообщений);
  - параметры отправки уведомлений получателю (с оригиналом сообщения или без него).
- Для новых параметров версии 2.0, отсутствовавших в версии 1.1 MR3, устанавливаются значения по умолчанию согласно таблице ниже.

Таблица 7. Значения по умолчанию для новых параметров версии 2.0

Параметр	Значение по умолчанию
Контентная фильтрация по формату вложения	**Вложения, тип которых указан в списке**
Проверка ссылок	• **Включено**. • Действие – **Отклонить**. • Метка – *[Malicious|Adware|Legitimate links]*. • Флажок **Поместить копию в Хранилище** установлен.
Предупреждение о небезопасном сообщении для сообщений, содержащих ссылки	**Отключено**

Настройка хранения экспортированных файлов

Вы можете ограничить количество экспортированных конфигурационных файлов, которые хранятся на сервере. В случае превышения установленного ограничения ранее экспортированные файлы будут удалены.

► *Чтобы настроить хранение экспортированных файлов:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Общие** → **Экспорт/импорт параметров**.
2. Выберите закладку **Экспорт**.
3. Нажмите на кнопку **Параметры хранения**.

   Откроется окно **Параметры хранения экспортированных файлов**.
4. В поле **Максимальное количество хранимых конфигурационных файлов** укажите максимальное количество экспортированных файлов, сохраняемых на сервере.

   Возможные значения: 1 – 2 147 483 647. По умолчанию установлено значение 50.

Количество экспортированных файлов будет ограничено заданным значением.

kaspersky

Интеграция с внешней службой каталогов

Kaspersky Secure Mail Gateway позволяет подключаться к серверам внешних служб каталогов, используемых в вашей организации, по протоколу LDAP.

Соединение с внешней службой каталогов по протоколу LDAP предоставляет администратору Kaspersky Secure Mail Gateway следующие возможности:

- Добавлять отправителей или получателей из внешней службы каталогов в правила обработки сообщений.
- Использовать функцию автодополнения полей **Email отправителя** и **Email получателя** при фильтрации копий сообщений пользователей локальной сети организации в Хранилище.

После настройки соединения с LDAP-сервером (см. раздел "Добавление соединения с LDAP-сервером" на стр. 225) программа выполняет автоматическую синхронизацию данных с контроллером домена Active Directory каждые 30 минут. Если вам требуется обновить данные об учетных записях пользователей немедленно (например, при добавлении нового пользователя), вы можете запустить синхронизацию вручную (см. раздел "Запуск синхронизации с контроллером домена Active Directory вручную" на стр. 227).

Каждый узел кластера выполняет синхронизацию самостоятельно, независимо от других узлов. В результате успешной синхронизации в LDAP-кеше сохраняется следующая информация:

- учетные записи всех пользователей домена;
- группы, в которых состоят пользователи домена;
- адреса электронной почты пользователей домена.

Программа хранит и использует эти данные до следующего запуска синхронизации. Если контроллер домена недоступен, используются последние полученные данные. После удаления соединения с LDAP-сервером (см. раздел "Удаление соединения с LDAP-сервером" на стр. 226) все данные LDAP-кеша удаляются.

В этом разделе

Создание keytab-файла

► *Чтобы создать keytab-файл:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя, которая будет использоваться для подключения программы к LDAP-серверу (например, с именем `ksmg-ldap`).

При создании пользователя требуется выбрать опцию **Password never expires**.

2. Чтобы использовать алгоритм шифрования AES256-SHA1, в оснастке **Active Directory Users and Computers** в свойствах созданной учетной записи на закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `ksmg-ldap` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ ksmg-ldap@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <пароль пользователя ksmg-ldap> -out <путь к файлу>\<имя файла>.keytab
   ```

   Вы можете использовать символ * в качестве значения параметра -pass, чтобы не указывать пароль в тексте команды. В этом случае утилита запросит пароль в процессе выполнения команды.

Пример:

```
C:\Windows\system32\ktpass.exe -princ ksmg-ldap@COMPANY.COM -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\Keytabs\ksmg-ldap.keytab
```

Keytab-файл будет создан. В случае изменения пароля учетной записи потребуется сгенерировать новый keytab-файл.

Добавление соединения с LDAP-сервером

Функциональность доступна только при наличии права **Изменять параметры**.

Вы можете добавить соединение с одним или несколькими LDAP-серверами.

► *Чтобы добавить соединение с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавить соединение**.
3. В поле **Название** введите имя, которое будет отображаться в веб-интерфейсе программы.

   Это имя не используется программой при взаимодействии с LDAP-сервером.

4. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 224).

   Откроется окно выбора файла.

5. Выберите keytab-файл и нажмите на кнопку **Open**.

   Keytab-файл должен содержать только одну запись с учетными данными пользователя Kaspersky Secure Mail Gateway, имеющего доступ к добавляемому домену.

6. В поле **База поиска** введите *DN* (*Distinguished Name* – уникальное имя) объекта каталога, начиная с которого Kaspersky Secure Mail Gateway осуществляет поиск записей.

7. Вводите суффикс каталога в формате `ou=<название подразделения>`(если требуется),`dc=<имя домена>,dc=<имя родительского домена>`.

   Например, вы можете ввести `ou=people,dc=example,dc=com`.

   Здесь `people` – уровень в схеме каталога, начиная с которого Kaspersky Secure Mail Gateway осуществляет поиск записей (поиск осуществляется на уровне `people` и ниже. Объекты, расположенные выше этого уровня, исключаются из поиска), `example` – доменное имя каталога, в котором Kaspersky Secure Mail Gateway осуществляет поиск записей, `com` – имя родительского домена, в котором находится каталог.

8. Нажмите на кнопку **Добавить**.

Соединение с LDAP-сервером будет добавлено.

Удаление соединения с LDAP-сервером

Вы можете удалить соединение с одним или несколькими LDAP-серверами.

► *Чтобы удалить соединение с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Выберите LDAP-сервер, который вы хотите удалить.

   Откроется окно **Просмотреть параметры соединения**.

3. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.

4. Нажмите на кнопку **ОК**.

Соединение с LDAP-сервером будет удалено. Синхронизация данных с контроллером домена будет прекращена. Из LDAP-кеша будут удалены данные об учетных записях пользователей, принадлежащих к этому домену.

kaspersky

Изменение параметров соединения с LDAP-сервером

► *Чтобы изменить параметры соединения с LDAP-сервером, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Выберите LDAP-сервер, параметры соединения с которым вы хотите изменить.

   Откроется окно **Просмотреть параметры соединения**.
3. Нажмите на кнопку **Изменить**.
4. Если требуется, измените следующие параметры:
   - Имя LDAP-сервера, которое отображается в веб-интерфейсе программы, в поле **Название**.
   - Keytab-файл, нажав на кнопку **Заменить**.
   - Каталог, начиная с которого программа осуществляет поиск записей, в поле **База поиска**.
5. Нажмите на кнопку **Сохранить**.

Параметры соединения с LDAP-сервером будут изменены.

Запуск синхронизации с контроллером домена Active Directory вручную

► *Чтобы запустить синхронизацию с контроллером домена Active Directory вручную, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Внешние службы** → **Подключения к LDAP-серверам**.
2. Нажмите на кнопку **Синхронизировать**.

Синхронизация данных с контроллером домена будет запущена. В результате будут обновлены данные об учетных записях пользователей, используемые при подборе правил и при автозаполнении имен пользователей в веб-интерфейсе программы.

Актуальный статус синхронизации с Active Directory отображается в разделе **Узлы** при просмотре информации об узлах кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130).

kaspersky

Защита KATA

Вы можете настроить интеграцию Kaspersky Secure Mail Gateway с Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform (KATA) – решение (далее также "программа"), предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (далее также "APT").

В результате интеграции Kaspersky Secure Mail Gateway сможет отправлять сообщения электронной почты на проверку Kaspersky Anti Targeted Attack Platform и получать результат проверки. KATA проверяет сообщения на наличие признаков целевых атак и вторжений в IT-инфраструктуру организации.

По результатам проверки KATA Kaspersky Secure Mail Gateway может блокировать отдельные сообщения.

Настройка интеграции Kaspersky Secure Mail Gateway с программой KATA состоит из следующих этапов.

a. **Добавление сервера KATA (на стр. 229)**

   При добавлении сервера KATA требуется сверить отпечатки сертификата, отображаемые в веб-интерфейсах Kaspersky Secure Mail Gateway и KATA. Если отпечатки совпадают, администратор подтверждает добавление сервера KATA. После этого Управляющий узел отправляет адрес и сертификат сервера KATA на все узлы кластера, не дожидаясь подтверждения авторизации.

b. **Настройка параметров защиты KATA (на стр. 229)**

   Вы можете настроить следующие параметры:

   - отправку на проверку в KATA всех сообщений или только сообщений, в которых по результатам проверки всеми модулями программы ничего не обнаружено;
   - время ожидания ответа от сервера KATA;
   - параметры KATA карантина.

c. **Авторизация Kaspersky Secure Mail Gateway в веб-интерфейсе программы KATA**

   Во время добавления сервера KATA отправляется запрос на авторизацию внешней системы. Администратору KATA требуется подтвердить в веб-интерфейсе KATA запрос на авторизацию от каждого узла кластера. Подробнее об обработке запросов от внешних систем см. *Справку Kaspersky Anti Targeted Attack Platform*.

d. **Проверка соединения с сервером KATA (см. раздел "Мониторинг интеграции с KATA" на стр. 230)**

В этом разделе

kaspersky

Добавление сервера KATA

Вы можете настроить интеграцию только с одним сервером KATA.

► *Чтобы добавить сервер KATA:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры**.
3. В блоке параметров **Сервер KATA** нажмите на кнопку **Добавление сервера KATA**.

   Откроется окно **Добавление сервера KATA**.
4. В поле **IP-адрес** введите полное доменное имя (FQDN) или IPv4-адрес сервера KATA, на котором установлен компонент Central Node.

   IPv6-адреса не поддерживаются.
5. В поле **Порт** введите порт подключения к серверу KATA.

   По умолчанию указано значение 443.
6. Нажмите на кнопку **Далее**.

   В поле **Отпечаток SHA256** отобразится отпечаток сертификата сервера KATA.
7. Проверьте введенные данные и убедитесь, что отпечаток сертификата, отображаемый в веб-интерфейсе, совпадает с отпечатком сертификата сервера KATA. Если отпечатки совпадают, нажмите на кнопку **Подтвердить**.

Сервер KATA будет добавлен. Информация о сервере отобразится в разделе **Защита KATA**, на закладке **Параметры** в блоке параметров **Сервер KATA**.

Настройка параметров защиты KATA

► *Чтобы настроить параметры защиты KATA:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Внешние службы** → **Защита KATA**.
2. Выберите закладку **Параметры**.
3. Если вы хотите отправлять на проверку в KATA сообщения, в которых по результатам проверки программой Kaspersky Secure Mail Gateway ничего не обнаружено, переведите переключатель **Отправлять на сервер KATA сообщения без обнаружений** в положение **Включено**.
4. Если вы хотите отправлять на проверку в KATA все сообщения, переведите переключатель **Отправлять на сервер KATA сообщения с обнаружениями** в положение **Включено**.

   Доступно только при включенном переключателе **Отправлять на сервер KATA сообщения без обнаружений**.

5. В поле **Максимальное время ожидания ответа от KATA (с)** введите максимальное время ожидания результата проверки сообщения от сервера KATA.

   При превышении указанного времени ожидания программа прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

   Возможные значения: 60 - 86400 (24 часа). Значение по умолчанию: 600

6. В поле **Максимальный размер KATA-карантина (МБ)** введите максимальный допустимый размер, занимаемый на диске KATA карантином, при превышении которого копии сообщений не будут помещаться в карантин.

   При превышении указанного размера программа прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

   Возможные значения: 1 - 8589934592. Значение по умолчанию: 1024

7. В поле **Максимальное количество сообщений в KATA-карантине** введите количество сообщений в KATA карантине, при превышении которого копии сообщений не будут помещаться в карантин.

   При превышении указанного количества программа прерывает проверку сообщения, присваивает ему статус *Пропущено* для модуля **KATA** и выполняет действие над сообщением без учета проверки сервером KATA.

   Возможные значения: 1 - 4294967296. Значение по умолчанию: 5000

8. Нажмите на кнопку **Сохранить**.

Параметры защиты KATA будут настроены.

Мониторинг интеграции с KATA

Чтобы отслеживать проблемы интеграции с KATA вы можете просматривать сводную информацию о состоянии подключения к серверу KATA на всех узлах кластера на информационной панели **Защита KATA** в разделе **Узлы**.

Возможны следующие статусы:

- *Подключено* – все узлы кластера успешно подключились и авторизованы на сервере KATA.
- *Ошибки* – хотя бы на одном узле кластера возникла хотя бы одна из следующих ошибок в течение последнего часа:
  - *Неавторизованное соединение*.
  - *Проблемы соединения*.
  - *Слишком много запросов авторизации*.
- *Отключено* – интеграция с KATA отключена в параметрах программы.

► *Чтобы просмотреть детальную информацию о состоянии подключения к серверу KATA на каждом узле кластера,*

по ссылке **Подробнее** на информационной панели **Защита KATA** перейдите в раздел **Параметры** → **Внешние службы** → **Защита KATA** → **Статус**.

В рабочей области отображается таблица узлов кластера с информацией о подключении к серверу KATA:

- **IP-адрес:порт** – IP-адрес и порт узла кластера.
- **Роль** – роль узла в кластере.
- **Отпечаток SHA256** – отпечаток сертификата сервера.
- **Статус** – состояние подключения к серверу KATA:
  - *Подключено* – узел кластера успешно подключен и авторизован на сервере KATA.
  - *Неавторизованное соединение* – подключение с сервером KATA установлено, но администратор KATA еще не подтвердил запрос на интеграцию.
  - *Проблемы соединения* – ошибка подключения к серверу KATA.
  - *Отключено* – интеграция с KATA отключена в параметрах программы.
  - *Слишком много запросов авторизации* – превышено максимальное количество запросов на интеграцию, установленное на сервере KATA.

    По умолчанию установлено значение 50.

Вы также можете просмотреть сведения о подключении к серверу KATA в окне с информацией о каждом узле кластера (см. раздел "Просмотр информации об узле кластера" на стр. 130).

kaspersky

Работа с программой по протоколу SNMP

SNMP (Simple Network Management Protocol – простой протокол сетевого управления) – протокол управления сетевыми устройствами.

В Kaspersky Secure Mail Gateway для работы по протоколу SNMP используется *SNMP-агент*, который отслеживает информацию о работе программы. Kaspersky Secure Mail Gateway может отправлять эту информацию в виде статистики, а также *SNMP-ловушек* – уведомлений о событиях работы программы.

По протоколу SNMP вы можете получить доступ к следующей информации о программе:

- общим сведениям;
- статистике работы Kaspersky Secure Mail Gateway с момента установки программы;
- данным о событиях, возникающих в ходе работы Kaspersky Secure Mail Gateway.

Доступ предоставляется только на чтение информации.

Информация об SNMP-ловушках и статистике, отправляемой по протоколу SNMP, хранится в базе данных MIB. В качестве SNMP-сервера, принимающего статистику, используется локальная служба snmpd на каждом узле кластера. Взаимодействие с внешним SNMP-сервером по протоколу AgentX не поддерживается. SNMP-ловушки можно принимать с помощью службы snmptrapd локально на каждом узле кластера или перенаправлять на внешний сервер.

Для работы по протоколу SNMP требуется предварительно настроить службу snmpd в операционной системе (см. раздел «Настройка службы snmpd в операционной системе» на стр. 235) на каждом узле кластера.

В этом разделе

kaspersky

Настройка шифрования SNMP-соединений

Сторонние программы могут получать доступ к данным, отправляемым по протоколу SNMP, или заменять эти данные своими данными. Для безопасной передачи данных по протоколу SNMP рекомендуется настроить шифрование SNMP-соединений.

► *Чтобы настроить шифрование SNMP-соединений, выполните следующие действия:*

1. Получите EngineID, необходимый для обработки SNMP-ловушек. Для этого на каждом сервере, входящем в кластер, выполните команду:

   ```
   snmpget -v2c -c<community name> 127.0.0.1 SNMP-FRAMEWORK-
   MIB::snmpEngineID.0 2>/dev/null | sed -ne 's/ //g; s/.*:/0x/p'
   ```

   Укажите имя сообщества (community name), которое используется в вашей организации. При необходимости создайте новое сообщество. В целях безопасности передачи данных не рекомендуется использовать сообщество public, заданное по умолчанию.

   Перед выполнением команды убедитесь, что служба snmpd запущена.

2. На каждом сервере входящем в кластер, настройте службу snmpd. Для этого выполните следующие действия:

   a. Остановите службу snmpd. Для этого выполните команду:

      ```
      systemctl stop snmpd
      ```

   b. Создайте нового пользователя. Для этого выполните команду:

      ```
      net-snmp-create-v3-user -ro -a SHA -A <password> -x <password> -X AES
      <username>
      ```

   c. Добавьте в конфигурационный файл /etc/snmp/snmpd.conf следующие строки:

      ```
      # accept KSMG statistics over unix socket

      master agentx

      agentXSocket unix:/var/run/agentx-master.socket

      agentXPerms 770 770 kluser klusers

      # accept incoming SNMP requests over UDP

      agentAddress udp:127.0.0.1:161

      rouser <username> priv .1.3.6.1

      # comment the following line if you don't need SNMP traps forwarding
      over SNMPv3 connection

      trapsess -e <EngineID> -v3 -l authPriv -u <username> -a SHA -A
      <password> -x AES -X <password> udp:<IP address>:162
      ```

> В качестве <IP address> укажите IP-адрес, по которому сервис snmptrapd будет принимать сетевые соединения. Если вы хотите сохранять SNMP-ловушки локально на сервере, укажите 127.0.0.1.

d. Добавьте в конфигурационный файл /etc/snmp/snmp.conf следующие строки:

```
mibdirs +/opt/kaspersky/ksmg/share/snmp-mibs/
mibs all
```

Если в указанной директории нет конфигурационного файла snmp.conf, вам необходимо его создать.

e. Запустите службу snmpd. Для этого выполните команду:

```
systemctl start snmpd
```

f. Проверьте SNMP-соединение. Для этого выполните следующие команды:

```
snmpwalk -mALL -v3 -l authPriv -u <username> -a SHA -A <password> -x AES -X <password> udp:127.0.0.1:161 .1.3.6.1.4.1.23668
```

```
snmpget -v3 -l authPriv -u <username> -a SHA -A <password> -x AES -X <password> udp:127.0.0.1:161 KSMG-PRODUCTINFO-STATISTICS::applicationName.0
```

3. На сервере, на котором вы хотите получать SNMP-ловушки, настройте службу snmptrapd. Для этого выполните следующие действия:

a. Остановите службу snmptrapd. Для этого выполните команду:

```
systemctl stop snmptrapd
```

b. Добавьте строку `createUser -e <EngineID> <username> SHA "<password>" AES "<password>"` в конфигурационный файл /var/lib/net-snmp/snmptrapd.conf.

Если в указанной директории нет конфигурационного файла snmptrapd.conf, вам необходимо его создать.

> Учетные данные пользователя (<username> и <password>) для служб snmpd и snmptrapd должны совпадать.

c. Добавьте в конфигурационный файл /etc/snmp/snmptrapd.conf следующие строки:

```
snmpTrapdAddr udp:<IP address>:162
authUser log <username> priv
disableAuthorization no
```

Если в указанной директории нет конфигурационного файла snmptrapd.conf, вам необходимо его создать.

d. Запустите службу snmptrapd. Для этого выполните команду:

```
systemctl start snmptrapd
```

Убедитесь, что пароль, указанный в файле /var/lib/net-snmp/snmptrapd.conf в открытом виде, заменен на обфусцированную последовательность символов. Для этого может потребоваться несколько раз перезапустить службу snmptrapd с помощью команды `systemctl restart snmptrapd`.

e. Добавьте службу snmptrapd в автозагрузку. Для этого выполните команду:

```
systemctl enable snmptrapd
```

f. Проверьте SNMP-соединение с помощью команды:

```
snmptrap -e <EngineID> -v3 -l authPriv -u <username> -a SHA -A
<password> -x AES -X <password> udp:<IP address>:162 0 KSMG-EVENTS-
MIB::restartedBinary
```

Убедитесь, что в файле /var/log/messages появляется следующая строка:

```
<date and time> <hostname> snmptrapd[7503]: <date and time> localhost
[UDP: [127.0.0.1]:26325->[<IP address>]:162]:#012DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks: (0) 0:00:00.00#011SNMPv2-
MIB::snmpTrapOID.0 = OID: KSMG-EVENTS-MIB::restartedBinary
```

В качестве `<IP address>` укажите IP-адрес, по которому сервис snmptrapd будет принимать сетевые соединения. Если вы хотите сохранять SNMP-ловушки локально на сервере, укажите `127.0.0.1`.

Шифрование SNMP-соединений будет настроено.

Настройка службы snmpd в операционной системе

Рекомендуемые параметры службы snmpd, заданные в конфигурационном файле /etc/snmp/snmpd.conf, описаны в инструкции по настройке шифрования SNMP-соединений (см. раздел "Настройка шифрования SNMP-соединений" на стр. 233).

► *Чтобы настроить службу snmpd, выполните следующие действия:*

1. Добавьте в файл /etc/snmp/snmpd.conf следующие строки для соединений через UNIX™-сокет:

```
master agentx
agentXSocket unix:/var/run/agentx-master.socket
agentXPerms 770 770 kluser klusers
```

2. Перезапустите службу snmpd. Для этого выполните команду:

```
systemctl restart snmpd
```

3. Добавьте службу snmpd в автозагрузку. Для этого выполните команду:

```
systemctl enable snmpd
```

Служба snmpd будет настроена. Для работы с программой по протоколу SNMP вам требуется включить его использование в веб-интерфейсе программы.

Если служба snmpd была настроена до установки Kaspersky Secure Mail Gateway, передача данных программы по протоколу SNMP может осуществляться некорректно. В этом случае требуется повторно перезапустить службу snmpd.

Включение и отключение использования SNMP в Kaspersky Secure Mail Gateway

Перед включением использования протокола SNMP требуется настроить службу snmpd в операционной системе (см. раздел "Настройка службы snmpd в операционной системе" на стр. 235).

► *Чтобы включить или отключить использование SNMP в работе программы:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите или отключите переключатель **Использовать SNMP**.
3. Нажмите на кнопку **Сохранить**.

Использование SNMP будет включено или отключено.

Настройка параметров подключения к SNMP-серверу

► *Чтобы настроить параметры подключения к SNMP-серверу:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите переключатель **Использовать SNMP**, если он отключен.
3. В поле **Путь к сокету**, укажите путь к файлу сокета.

   По умолчанию указан путь `/var/run/agentx-master.socket`.

   Для подключения к SNMP-серверу используется UNIX-сокет. Использование TCP- и UDP-сокетов не поддерживается.

4. В поле **Время ожидания ответа сервера (с)** укажите максимальное время ожидания ответа от SNMP-сервера в секундах. Вы можете указать значение в интервале от 1 до 255 секунд.

   Значение по умолчанию: 15 секунд.

5. Нажмите на кнопку **Сохранить**.

Параметры подключения к SNMP-серверу будут настроены.

Включение и отключение отправки SNMP-ловушек

► *Чтобы включить или отключить отправку SNMP-ловушек событий, возникающих в ходе работы программы:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Мониторинг** → **SNMP**.
2. Включите или отключите переключатель **Отправлять SNMP-ловушки**.

   Опция доступна только при включенном переключателе **Использовать SNMP**.

Отправка SNMP-ловушек будет включена или отключена. Программа будет отправлять SNMP-ловушки при наступлении событий, соответствующих объектам MIB (см. раздел "Описание объектов MIB Kaspersky Secure Mail Gateway" на стр. 237).

Описание объектов MIB Kaspersky Secure Mail Gateway

В таблице ниже приведена информация об объектах MIB Kaspersky Secure Mail Gateway.

kaspersky

События в работе программы

Таблица 8. События в работе программы

Символьное имя	Описание	Параметры	Идентификатор (OID)
updateErrorEvent	Обновление баз программы завершилось ошибкой.	• FQDN узла, на котором произошло событие. • Причина ошибки.	.1.3.6.1.4.1.23668.1735.1.10
aspBasesCompilationFailedEvent	Компиляция баз модуля Анти-Спам завершилась ошибкой.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.30
avBasesOutdatedEvent	Базы модуля Антивирус устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.100
avBasesObsoletedEvent	Базы модуля Антивирус сильно устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.120
aspBasesOutdatedEvent	Базы модуля Анти-Спам устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.130
aspBasesObsoletedEvent	Базы модуля Анти-Спам сильно устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.140
apBasesOutdatedEvent	Базы модуля Анти-Фишинг устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.150
apBasesObsoletedEvent	Базы модуля Анти-Фишинг сильно устарели.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.160

Символьное имя	Описание	Параметры	Идентификатор (OID)
backupAddErrorEvent	Ошибка добавления резервной копии.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения. • Причина ошибки.	.1.3.6.1.4.1.23668.1735.1.200
backupRotateErrorEvent	Ошибка удаления резервных копий из Хранилища.	• FQDN узла, на котором произошло событие. • Причина ошибки.	.1.3.6.1.4.1.23668.1735.1.210
backupLimitReachedEvent	Достигнут максимально допустимый объем Хранилища.	• FQDN узла, на котором произошло событие. • Количество сообщений. • Суммарный размер сообщений. • Максимально допустимый объем Хранилища.	.1.3.6.1.4.1.23668.1735.1.220
licenseInstalledEvent	Код активации или файл ключа добавлен.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии.	.1.3.6.1.4.1.23668.1735.1.300

Символьное имя	Описание	Параметры	Идентификатор (OID)
licenseUpdatedEvent	Статус лицензионного ключа изменен.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии. • Тип лицензии. • Тип функциональности. • Дата окончания срока действия лицензии.	.1.3.6.1.4.1.23668.1735.1.360
gracePeriodEvent	Начался льготный период действия лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии. • Количество дней до завершения льготного периода.	.1.3.6.1.4.1.23668.1735.1.380
licenseRevokedEvent	Код активации или файл ключа удален.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии.	.1.3.6.1.4.1.23668.1735.1.310
licenseExpiresSoonEvent	Срок действия лицензии скоро истечет.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии. • Количество дней до окончания срока действия лицензии.	.1.3.6.1.4.1.23668.1735.1.320

Символьное имя	Описание	Параметры	Идентификатор (OID)
licenseExpiredEvent	Истек срок действия лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии. • Дата окончания срока действия лицензии.	.1.3.6.1.4.1.23668.1735.1.330
licenseTrialPeriodIsOverEvent	Истек срок действия пробной лицензии.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии. • Дата окончания срока действия лицензии.	.1.3.6.1.4.1.23668.1735.1.340
licenseBlacklistedEvent	Код активации или файл ключа помещен в список запрещенных.	• FQDN узла, на котором произошло событие. • Серийный номер лицензии.	.1.3.6.1.4.1.23668.1735.1.350
taskCrashEvent	Процесс программы завершился аварийно.	• FQDN узла, на котором произошло событие. • Полный путь к бинарному файлу.	.1.3.6.1.4.1.23668.1735.1.400
taskRestartEvent	Процесс программы перезапущен.	• FQDN узла, на котором произошло событие. • Полный путь к бинарному файлу.	.1.3.6.1.4.1.23668.1735.1.410

Символьное имя	Описание	Параметры	Идентификатор (OID)
productStartEvent	Программа запущена. Это событие возникает после того, как запускаются все службы, необходимые для работы Kaspersky Secure Mail Gateway.	• FQDN узла, на котором произошло событие.	.1.3.6.1.4.1.23668.1735.1.420
threatDetectedEvent	Обнаружена угроза.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Статус модуля Антивирус. • Список обнаруженных объектов.	.1.3.6.1.4.1.23668.1735.1.510
antiVirusErrorEvent	Ошибка модуля Антивирус.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Причина ошибки.	.1.3.6.1.4.1.23668.1735.1.520
antiSpamErrorEvent	Ошибка модуля Анти-Спам.	• FQDN узла, на котором произошло событие. • Идентификатор сообщения на почтовом сервере. • Причина ошибки.	.1.3.6.1.4.1.23668.1735.1.530

Символьное имя	Описание	Параметры	Идентификатор (OID)
ksnConnectionStatusEvent	Изменилось состояние соединения с сервером KSN.	• FQDN узла, на котором произошло событие. • Новое состояние соединения с сервером KSN.	.1.3.6.1.4.1.23668.1735.1.700
clusterConsistencyErrorEvent	Ошибка состояния серверов. Например, нет ни одного сервера с ролью Управляющий узел.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.	.1.3.6.1.4.1.23668.1735.1.1600
clusterEmergencyStateEvent	Программа перешла в аварийный режим.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.	.1.3.6.1.4.1.23668.1735.1.1610
settingsSynchronizationErrorEvent	Ошибка синхронизации параметров между Управляющим и Подчиненными узлами.	• FQDN узла, на котором произошло событие. • Сообщение об ошибке.	.1.3.6.1.4.1.23668.1735.1.1620
ldapCacheUpdateEvent	Синхронизация данных с Active Directory завершена.	• FQDN узла, на котором произошло событие. • Статус синхронизации LDAP-кэша. • Статус синхронизации данных для автозаполнения учетных записей.	.1.3.6.1.4.1.23668.1735.1.910

Статистика модуля Антивирус

Таблица 9. Статистика модуля Антивирус

Символьное имя	Описание	Идентификатор (OID)
antivirusStatistics.notDetectedMessages	Количество проверенных собщений, в которых не обнаружены угрозы.	.1.3.6.1.4.1.23668.1735.2.2.1.0
antivirusStatistics.infectedMessages	Количество сообщений, в которых обнаружены угрозы.	.1.3.6.1.4.1.23668.1735.2.2.2.0
antivirusStatistics.encryptedMessages	Количество сообщений, для которых не удалось проверить зашифрованные (защищенные паролем) вложения.	.1.3.6.1.4.1.23668.1735.2.2.4.0

Символьное имя	Описание	Идентификатор (OID)
antivirusStatistics.docWithMacroMessages	Количество сообщений, содержащих вложения с макросами.	.1.3.6.1.4.1.23668.1735.2.2.5.0
antivirusStatistics.scanErrors	Количество сообщений, при обработке которых произошли ошибки.	.1.3.6.1.4.1.23668.1735.2.2.6.0
antivirusStatistics.notScannedSettingsMessages	Количество сообщений, которые не были проверены на наличие угроз согласно заданным значениям параметров для модуля Антивирус.	.1.3.6.1.4.1.23668.1735.2.2.7.0
antivirusStatistics.notScannedViolationsMessages	Количество сообщений, которые не были проверены на наличие угроз из-за проблем, связанных с лицензией или базами программы.	.1.3.6.1.4.1.23668.1735.2.2.8.0

Статистика антивирусных баз

Таблица 10. Статистика антивирусных баз

Символьное имя	Описание	Идентификатор (OID)
antivirusbasesStatistics.basesDate	Дата и время последнего обновления антивирусных баз.	.1.3.6.1.4.1.23668.1735.2.6.1.0
antivirusbasesStatistics.basesRecordCount	Количество записей в антивирусных базах.	.1.3.6.1.4.1.23668.1735.2.6.2.0
antivirusbasesStatistics.basesStatus	Текущее состояние антивирусных баз.	.1.3.6.1.4.1.23668.1735.2.6.3.0

Статистика Проверки ссылок

Таблица 11. Статистика Проверки ссылок

Символьное имя	Описание	Идентификатор (OID)
linksScanning.notDetectedMessages	Количество проверенных сообщений, в которых не обнаружены ссылки.	.1.3.6.1.4.1.23668.1735.2.12.1.0
linksScanning.linksScanningMessages	Количество сообщений, в которых обнаружены вредоносные, рекламные ссылки или ссылки, связанные с легальными программами, которые могут быть использованы злоумышленниками.	.1.3.6.1.4.1.23668.1735.2.12.3.0

Символьное имя	Описание	Идентификатор (OID)
linksScanning.scanErrors	Количество сообщений, при обработке которых произошли ошибки.	.1.3.6.1.4.1.23668.1735.2.12.4.0
linksScanning.notScannedSettingsMessages	Количество сообщений, которые не были проверены на наличие ссылок согласно заданным значениям параметров для Проверки ссылок.	.1.3.6.1.4.1.23668.1735.2.12.5.0
linksScanning.notScannedViolationsMessages	Количество сообщений, которые не были проверены на наличие ссылок из-за проблем, связанных с лицензией или базами программы.	.1.3.6.1.4.1.23668.1735.2.12.6.0

Статистика модуля Анти-Спам

Таблица 12. Статистика модуля Анти-Спам

Символьное имя	Описание	Идентификатор (OID)
antispamStatistics.notDetectedMessages	Количество проверенных сообщений, в которых не обнаружен спам.	.1.3.6.1.4.1.23668.1735.2.3.1.0
antispamStatistics.spamMessages	Количество сообщений, в которых обнаружен спам.	.1.3.6.1.4.1.23668.1735.2.3.2.0
antispamStatistics.probableSpamMessages	Количество сообщений, в которых обнаружен предполагаемый спам.	.1.3.6.1.4.1.23668.1735.2.3.3.0
antispamStatistics.denylistedMessages	Количество отклоненных сообщений с серверов, которые были добавлены в список запрещенных адресов.	.1.3.6.1.4.1.23668.1735.2.3.4.0
antispamStatistics.antiSpamQuarantinedMessages	Количество сообщений, помещенных в Анти-Спам карантин.	.1.3.6.1.4.1.23668.1735.2.3.5.0
antispamStatistics.scanErrors	Количество сообщений, при обработке которых произошли ошибки.	.1.3.6.1.4.1.23668.1735.2.3.6.0

Символьное имя	Описание	Идентификатор (OID)
antispamStatistics.notScannedSettingsMessages	Количество сообщений, которые не были проверены на наличие спама согласно заданным значениям параметров для модуля Анти-Спам.	.1.3.6.1.4.1.23668.1735.2.3.7.0
antispamStatistics.notScannedViolationsMessages	Количество сообщений, которые не были проверены на наличие спама из-за проблем, связанных с лицензией или базами программы.	.1.3.6.1.4.1.23668.1735.2.3.8.0
antispamStatistics.massMail	Количество сообщений, признанных массовой рассылкой.	.1.3.6.1.4.1.23668.1735.2.3.9.0

Статистика баз модуля Анти-Спам

Таблица 13. Статистика баз модуля Анти-Спам

Символьное имя	Описание	Идентификатор (OID)
antispambasesStatistics.basesDate	Дата и время последнего обновления баз модуля Анти-Спам.	.1.3.6.1.4.1.23668.1735.2.7.1.0
antispambasesStatistics.basesStatus	Текущее состояние баз модуля Анти-Спам.	.1.3.6.1.4.1.23668.1735.2.7.2.0

Статистика модуля Анти-Фишинг

Таблица 14. Статистика модуля Анти-Фишинг

Символьное имя	Описание	Идентификатор (OID)
antiphishingStatistics.notDetectedMessages	Количество проверенных сообщений, в которых не обнаружен фишинг.	.1.3.6.1.4.1.23668.1735.2.10.1.0
antiphishingStatistics.phishingMessages	Количество сообщений, в которых обнаружен фишинг.	.1.3.6.1.4.1.23668.1735.2.10.2.0
antiphishingStatistics.scanErrors	Количество сообщений, при обработке которых произошли ошибки.	.1.3.6.1.4.1.23668.1735.2.10.4.0
antiphishingStatistics.notScannedSettingsMessages	Количество сообщений, которые не были проверены на наличие фишинга согласно заданным значениям параметров для модуля Анти-Фишинг.	.1.3.6.1.4.1.23668.1735.2.10.5.0

Символьное имя	Описание	Идентификатор (OID)
antiphishingStatistics.notScannedViolationsMessages	Количество сообщений, которые не были проверены на наличие фишинга из-за проблем, связанных с лицензией или базами программы.	.1.3.6.1.4.1.23668.1735.2.10.6.0

Статистика баз модуля Анти-Фишинг

Таблица 15. Статистика баз модуля Анти-Фишинг

Символьное имя	Описание	Идентификатор (OID)
antiphishingbasesStatistics.basesDate	Дата и время последнего обновления баз модуля Анти-Фишинг.	.1.3.6.1.4.1.23668.1735.2.11.1.0
antiphishingbasesStatistics.basesStatus	Текущее состояние баз модуля Анти-Фишинг.	.1.3.6.1.4.1.23668.1735.2.11.2.0

Статистика контентной фильтрации

Таблица 16. Статистика контентной фильтрации

Символьное имя	Описание	Идентификатор (OID)
cfStatistics.notDetectedMessages	Количество проверенных объектов, к которым не были применены никакие действия.	.1.3.6.1.4.1.23668.1735.2.4.1.0

Символьное имя	Описание	Идентификатор (OID)
cfStatistics.sizeExceededMessages	Количество объектов, размер которых превышает максимальный допустимый размер, заданный в параметрах контентной фильтрации.	.1.3.6.1.4.1.23668.1735.2.4.2.0
cfStatistics.prohibitedTypeMessages	Количество сообщений, содержащих вложения запрещенного формата.	.1.3.6.1.4.1.23668.1735.2.4.3.0
cfStatistics.prohibitedNameMessages	Количество сообщений, содержащих вложения с запрещенными именами.	.1.3.6.1.4.1.23668.1735.2.4.4.0
cfStatistics.notScannedSettingsMessages	Количество сообщений, для которых не осуществлялась контентная фильтрация согласно заданным значениям параметров.	.1.3.6.1.4.1.23668.1735.2.4.5.0
cfStatistics.notScannedViolationsMessages	Количество сообщений, для которых не осуществлялась контентная фильтрация из-за проблем, связанных с лицензией или базами программы.	.1.3.6.1.4.1.23668.1735.2.4.6.0

Статистика примененных действий

Таблица 17. Статистика примененных действий

Символьное имя	Описание	Идентификатор (OID)
actionStatistics.notDetectedMessages	Количество сообщений, к которым не были применены никакие действия по результатам проверки всех включенных модулей программы.	.1.3.6.1.4.1.23668.1735.2.5.1.0
actionStatistics.disinfectedMessages	Количество вылеченных сообщений.	.1.3.6.1.4.1.23668.1735.2.5.2.0
actionStatistics.attachmentDeletedMessages	Количество сообщений, в которых были удалены зараженные вложения.	.1.3.6.1.4.1.23668.1735.2.5.3.0
actionStatistics.deletedMessages	Количество удаленных сообщений.	.1.3.6.1.4.1.23668.1735.2.5.4.0
actionStatistics.rejectedMessages	Количество отклоненных сообщений.	.1.3.6.1.4.1.23668.1735.2.5.5.0
actionStatistics.quarantinedMessages	Количество сообщений, помещенных на карантин, так как их обработка была отложена.	.1.3.6.1.4.1.23668.1735.2.5.6.0
actionStatistics.skippedMessages	Количество сообщений, не проверенных ни одним модулем из-за ошибок проверки.	.1.3.6.1.4.1.23668.1735.2.5.7.0

Символьное имя	Описание	Идентификатор (OID)
actionStatistics.unprocessedMessages	Количество сообщений, не проверенных ни одним модулем из-за недоступности баз программы.	.1.3.6.1.4.1.23668.1735.2.5.8.0

Статистика программы

Таблица 18. Статистика программы

Символьное имя	Описание	Идентификатор (OID)
productinfoStatistics.applicationName	Название программы.	.1.3.6.1.4.1.23668.1735.2.8.1.0
productinfoStatistics.applicationVersion	Версия программы.	.1.3.6.1.4.1.23668.1735.2.8.2.0
productinfoStatistics.installDate	Дата и время установки программы.	.1.3.6.1.4.1.23668.1735.2.8.3.0
productinfoStatistics.licenseExpireDate	Дата и время истечения срока действия лицензии.	.1.3.6.1.4.1.23668.1735.2.8.4.0
productinfoStatistics.licenseStatus	Текущее состояние лицензионного ключа.	.1.3.6.1.4.1.23668.1735.2.8.5.0

Статистика отчетов

Таблица 19. Статистика отчетов

Символьное имя	Описание	Идентификатор (OID)
reportsummaryStatistics.threatNumber	Количество сообщений, в которых обнаружены угрозы.	.1.3.6.1.4.1.23668.1735.2.9.1.0
reportsummaryStatistics.threatSize	Общий размер сообщений, в которых обнаружены угрозы.	.1.3.6.1.4.1.23668.1735.2.9.2.0
reportsummaryStatistics.spamNumber	Количество сообщений, в которых обнаружен спам.	.1.3.6.1.4.1.23668.1735.2.9.3.0
reportsummaryStatistics.spamSize	Общий размер сообщений, в которых обнаружен спам.	.1.3.6.1.4.1.23668.1735.2.9.4.0
reportsummaryStatistics.contentFilteringDetectsNumber	Количество сообщений, отклоненных согласно параметрам контентной фильтрации.	.1.3.6.1.4.1.23668.1735.2.9.5.0
reportsummaryStatistics.contentFilteringDetectsSize	Общий размер сообщений, отклоненных согласно параметрам контентной фильтрации.	.1.3.6.1.4.1.23668.1735.2.9.6.0
reportsummaryStatistics.notScannedNumber	Количество непроверенных сообщений.	.1.3.6.1.4.1.23668.1735.2.9.7.0

Символьное имя	Описание	Идентификатор (OID)
reportsummaryStatistics.notScannedSize	Общий размер непроверенных сообщений.	.1.3.6.1.4.1.23668.1735.2.9.8.0
reportsummaryStatistics.notDetectedNumber	Количество проверенных сообщений, в которых ничего не обнаружено.	.1.3.6.1.4.1.23668.1735.2.9.9.0
reportsummaryStatistics.notDetectedSize	Общий размер проверенных сообщений, в которых ничего не обнаружено.	.1.3.6.1.4.1.23668.1735.2.9.10.0
reportsummaryStatistics.totalNumber	Количество всех обработанных сообщений.	.1.3.6.1.4.1.23668.1735.2.9.11.0
reportsummaryStatistics.totalSize	Общий размер всех обработанных сообщений.	.1.3.6.1.4.1.23668.1735.2.9.12.0
reportsummaryStatistics.phishingNumber	Количество сообщений, содержащих фишинг.	.1.3.6.1.4.1.23668.1735.2.9.13.0
reportsummaryStatistics.phishingSize	Общий размер сообщений, содержащих фишинг.	.1.3.6.1.4.1.23668.1735.2.9.14.0

Статистика Хранилища

Таблица 20. Статистика Хранилища

Символьное имя	Описание	Идентификатор (OID)
backupStatistics.messageCount	Количество объектов, находящихся в Хранилище в данный момент.	.1.3.6.1.4.1.23668.1735.2.1.1.0
backupStatistics.usedSpace	Объем дискового пространства, занимаемый Хранилищем.	.1.3.6.1.4.1.23668.1735.2.1.2.0

Экспорт объектов MIB

► *Чтобы экспортировать файлы, содержащие информацию об объектах MIB:*

1. В веб-интерфейсе программы добавьте открытый ключ SSH (см. раздел "Добавление открытого ключа SSH" на стр. 276) для подключения к узлу кластера в режиме Technical Support Mode.
2. Выполните одну из следующих команд в зависимости от операционной системы на узле:
   - Windows:

     ```
     pscp -i <ppk_file_path> -r
     root@<hostname>:/opt/kaspersky/ksmg/share/snmp-mibs .
     ```

     Для выполнения этой команды требуется предварительно установить утилиту PuTTY.

   - Linux®:

     ```
     scp -r root@<hostname>:/opt/kaspersky/ksmg/share/snmp-mibs .
     ```

Файлы с информацией об объектах MIB будут экспортированы и сохранены в каталоге snmp-mibs в текущей директории.

kaspersky

Почтовые уведомления Kaspersky Secure Mail Gateway

Уведомления о событиях в работе программы (далее также "системные уведомления") содержат информацию о параметрах программы, ошибках, возникающих во время работы программы, а также о восстановлении программы после сбоев.

Вы можете настроить отправку системных уведомлений (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 263) администратору почтового сервера о следующих событиях в работе программы:

- Защита:
  - Антивирусные базы устарели.
  - Базы Анти-Спама устарели.
  - Базы Анти-Фишинга устарели.
  - Проблемы с обновлением баз.
  - Проблемы со службой KSN/KPSN.
  - Запросы KSN отфильтрованы.
- Синхронизация:
  - Узел недоступен.
  - Не удалось синхронизировать данные.
  - Не удалось применить значения параметров.
  - Время не совпадает со временем на Управляющем узле.
  - Проблемы конфигурации кластера.
- Интеграция LDAP:
  - Проблемы подключения к LDAP.
  - Не удалось сохранить данные LDAP для сопоставления правил.
  - Не удалось сохранить данные LDAP для автозаполнения учетных записей.

Текст уведомления содержит следующую информацию:

- Название группы и список ошибок, возникших на момент отправки уведомления.
- Дата и время последнего возникновения каждой ошибки.

  Для ошибок из групп **Синхронизация** и **Интеграция LDAP** также указывается дата и время последней успешной синхронизации.
- IP-адрес и порт подключения к узлу кластера, на котором возникли указанные ошибки.
- Комментарий к узлу кластера.

Программа отправляет системные уведомления один раз в сутки в 00:00 по локальному времени Управляющего узла, если на этот момент есть хотя бы одна из перечисленных выше ошибок. При возникновении новых ошибок и при исправлении имевшихся ранее ошибок программа отправляет системные уведомления не чаще, чем один раз в 15 минут.

kaspersky

Уведомления о срабатывании правил обработки сообщений содержат информацию об объектах, обнаруженных одним или несколькими модулями программы в результате проверки сообщения.

Вы можете настроить отправку уведомлений (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 264) отправителю и получателям сообщения, адресатам из дополнительного списка, заданного в сработавшем правиле, а также получателям из общего списка для всех правил. Для каждой из перечисленных групп получателей вы можете настроить разные шаблоны уведомлений (см. раздел "Настройка шаблонов уведомлений" на стр. 265).

В этом разделе

Настройка уведомлений о событиях в работе программы

Доступно только при наличии права **Изменять параметры**.

► *Чтобы настроить отправку уведомлений о событиях в работе программы:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Мониторинг** → **Системные уведомления**.
2. Включите или отключите отправку уведомлений о событиях в работе программы с помощью переключателя **Отправлять системные уведомления**.
3. Если на предыдущем шаге вы включили отправку уведомлений, в блоке параметров **Параметры уведомлений** нажмите на кнопку **Добавить**.
4. В появившемся поле **Адреса** введите адрес электронной почты и нажмите клавишу **ENTER**.

   Адреса электронной почты вводятся по одному. Повторите действия по добавлению адресов в список для всех добавляемых адресов электронной почты.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

   Регулярные выражения нечувствительны к регистру.

5. В раскрывающемся списке **Язык** выберите, на каком языке будет отображаться текст уведомления.

6. Если требуется, повторите шаги 5-6, чтобы добавить адресатов уведомлений на другом языке.
7. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о событиях в работе программы будет настроена.

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от программы" на стр. 269), который указывается в качестве отправителя уведомлений о событиях в работе программы.

Настройка уведомлений о срабатывании правил обработки сообщений

Доступно только при наличии права **Изменять параметры**.

Убедитесь, что отправка уведомлений включена в правиле (см. раздел "Настройка уведомлений о событиях проверки сообщений" на стр. 117), о срабатывании которого вы хотите получать уведомления.

► *Чтобы настроить отправку уведомлений о срабатывании правил обработки сообщений:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Перейдите по ссылке **Уведомления об обнаружениях**.

   Откроется окно **Уведомления об обнаружениях**.
3. Включите или отключите отправку уведомлений о событиях в работе программы с помощью переключателя **Отправлять уведомления об обнаружениях**.
4. Если на предыдущем шаге вы включили отправку уведомлений, в поле **Общий список получателей** введите адрес электронной почты и нажмите клавишу **ENTER**.

   Вы можете ввести сразу несколько адресов, разделенных точкой с запятой.

   Вы можете использовать символы "*" и "?" для создания масок адресов и регулярные выражения, начинающиеся с префикса "reg:".

   Регулярные выражения нечувствительны к регистру.
5. Нажмите на кнопку **Сохранить**.

Отправка уведомлений о срабатывании правил обработки сообщений будет настроена. Программа будет отправлять уведомления на указанные адреса в зависимости от параметров, заданных в сработавшем правиле:

- адресатам из общего списка, если в правиле установлен флажок **Уведомить получателей из общего списка**;
- отправителю сообщения, если в правиле установлен флажок **Уведомить отправителя**;

- получателям сообщения, если в правиле установлен флажок **Уведомить получателя**;
- на дополнительные адреса, если в правиле установлен флажок **Дополнительные адреса**.

Вы можете изменить заданный по умолчанию адрес (см. раздел "Настройка адреса сообщений от программы" на стр. 269), который указывается в качестве отправителя уведомлений о срабатывании правил обработки сообщений.

Настройка шаблонов уведомлений

Изменение шаблонов доступно только для уведомлений о срабатывании правила. Вы не можете изменить текст системных уведомлений.

Вы можете настроить разные шаблоны уведомлений для адресатов из общего списка, отправителя сообщения, получателей сообщения и адресатов из списка дополнительных адресов, заданных в правиле.

По умолчанию тексты шаблонов написаны на английском языке. Автоматическое переключение языков для шаблонов недоступно. Если требуется, вы можете переписать текст на нужном языке. Если вам нужно отправлять уведомления на разных языках в рамках одной группы получателей, вы можете написать один и тот же текст на нескольких языках и расположить их друг за другом в одном шаблоне.

► *Чтобы настроить шаблоны уведомлений:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. Перейдите по ссылке **Уведомления об обнаружениях**.

   Откроется окно **Уведомления об обнаружениях**.
3. По ссылке **Изменить шаблон** напротив нужного получателя откройте окно изменения шаблона.
4. Если требуется, в поле **Тема** измените тему уведомления.
5. Если требуется, в текстовой области **Тело сообщения** измените текст уведомления.

   Вы можете использовать макросы в теме и тексте сообщения. Для этого нажмите на кнопку **Добавить макрос** и выберите нужный макрос из раскрывающегося списка.

   > Значения макросов автоматически подставляются на английском языке. Переключение языков для макросов недоступно.
6. Нажмите на кнопку **Сохранить**.
7. Повторите шаги 3-6 для каждого шаблона.

Шаблоны уведомлений будут настроены.

Использование макросов в шаблонах уведомлений

Макрос – это элемент подстановки, используемый в шаблонах уведомлений о событиях. В формируемом на основе шаблона тексте уведомления макрос заменяется на некоторое значение.

Синтаксис макроса: `%ИМЯ_МАКРОСА%`

В текстах уведомлений о срабатывании правила можно использовать следующие макросы (см. таблицу ниже).

Таблица 21. Макросы для шаблонов уведомлений

Макрос	Описание
%NODE_IP%	IP-адрес узла кластера, на котором было обработано сообщение.
%NODE_PORT%	Порт подключения к узлу кластера, на котором было обработано сообщение.
%PRODUCT_NAME%	Название программы – Kaspersky Secure Mail Gateway.
%SMTP_MESSAGE_ID%	Заголовок сообщения `Message-Id`.
%SENDER%	Адрес отправителя сообщения.
%ALL_RECIPIENTS%	Адреса всех получателей исходного сообщения.
%AFFECTED_RECIPIENTS%	Адреса получателей исходного сообщения, имеющие отношение к событию, описанному в уведомлении.
%AFFECTED_RULES%	Список идентификаторов сработавших правил.
%MESSAGE_ID%	Идентификатор, присвоенный сообщению программой Kaspersky Secure Mail Gateway.
%SUBJECT%	Тема исходного сообщения.
%DATE%	Дата получения сообщения.
%MESSAGE_ACTION%	Действие программы над сообщением. Возможные значения: • `Skipped`. • `Disinfected`. • `AttachmentDeleted`. • `Deleted`. • `Rejected`. Если сообщение помещено в Хранилище, то через запятую после действия указывается `backed up`.

Макрос	Описание
%DATA_BEGIN%	Служебный макрос для обозначения начала списка вложений.
%DATA_END%	Служебный макрос для обозначения конца списка вложений.
%OBJECT_NAME%	Имя обнаруженного объекта. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляется имя вложения сообщения; • вне макросов %DATA_BEGIN% и %DATA_END% подставляется значение `Message`. В теме уведомления на место макроса всегда подставляется значение `Message`.
%OBJECT_SIZE%	Размер сообщения целиком или отдельных его вложений. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляется размер вложения сообщения; • вне макросов %DATA_BEGIN% и %DATA_END% подставляется размер сообщения целиком. В теме уведомления на место макроса всегда подставляется размер сообщения целиком.
%STATUS%	Результат проверки сообщения или вложения. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляются статусы проверки вложений модулями Антивирус и Контентная фильтрация; • вне макросов %DATA_BEGIN% и %DATA_END% подставляются статусы, присвоенные по результатам проверки сообщению целиком (если для этих статусов включена отправка уведомлений в правиле). В теме уведомления на место макроса всегда подставляются статусы, присвоенные по результатам проверки сообщению целиком (если для этих статусов включена отправка уведомлений в правиле). Если статусов несколько, они перечисляются через запятую.

Макрос	Описание
%OBJECT_ACTION%	Действие программы над сообщением или вложением. В теле уведомления значение макроса зависит от его расположения: • между макросами %DATA_BEGIN% и %DATA_END% подставляются действия над вложениями, выполненные модулями Антивирус или Контентная фильтрация (`Blocked`, `Not blocked`, `Disinfected`), или действие над сообщением целиком, выполненное модулем Анти-Фишинг. • вне макросов %DATA_BEGIN% и %DATA_END% подставляется действие, выполненное над сообщением целиком. В теме уведомления на место макроса всегда подставляется действие, выполненное над сообщением целиком.

Добавление в уведомление уникального идентификатора сообщения

Если пользователь получил уведомление об отклоненном сообщении, он может обратиться к администратору программы за более подробной информацией. В этом случае потребуется найти исходное письмо в Хранилище. Чтобы оптимизировать поиск, вы можете добавить уникальный идентификатор сообщения (далее также "ID сообщения") в шаблон уведомления.

► *Чтобы добавить ID сообщения в текст уведомления, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Правила**.
2. В таблице правил выберите правило, для которого вы хотите настроить уведомления о событиях проверки.

   Откроется окно **Просмотреть правило**.
3. В левой панели выберите раздел **Уведомления**.
4. Убедитесь, что флажки напротив нужных получателей уведомлений установлены. При необходимости внесите изменения и нажмите на кнопку **Сохранить**.
5. Перейдите по ссылке **Настроить шаблоны уведомлений** в правом верхнем углу окна.

   Откроется окно **Уведомления об обнаружениях**.
6. По ссылке **Изменить шаблон** напротив нужного получателя откройте окно настройки шаблона уведомления.
7. Добавьте в шаблон следующую строку:

   ```
   Message ID: %SMTP_MESSAGE_ID%
   ```
8. Нажмите на кнопку **Сохранить**.

Макрос для ID сообщения будет добавлен в шаблон уведомления. В тексте последующих уведомлений будет указан уникальный идентификатор сообщения.

kaspersky

Настройка адреса сообщений от программы

Вы можете указать адрес электронной почты, который будет указан в качестве отправителя следующих сообщений от программы:

- уведомлений о срабатывании правил (см. раздел "Настройка уведомлений о срабатывании правил обработки сообщений" на стр. 264);
- уведомлений о событиях в работе программы (см. раздел "Настройка уведомлений о событиях в работе программы" на стр. 263);
- сообщений из Хранилища, отправленных в виде вложения (см. раздел "Доставка сообщения из Хранилища" на стр. 160);
- отчетов (см. стр. 183);
- уведомлений о недоставке сообщений в случае применения программой действия **Отклонить**.

► *Чтобы настроить адрес сообщений от программы:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Мониторинг** → **Обратный адрес**.
2. В поле **Обратный адрес** укажите адрес, который будет отображаться в поле *От кого* в сообщениях от программы.

   Можно указать только один адрес.

   По умолчанию установлено значение `ksmg@<FQDN Управляющего узла кластера>`.
3. Нажмите на кнопку **Сохранить**.

Адрес сообщений от программы будет настроен.

kaspersky

Аутентификация с помощью технологии единого входа

При включении технологии единого входа пользователям не требуется вводить данные учетной записи программы для подключения к веб-интерфейсу. Аутентификация осуществляется с помощью доменной учетной записи пользователя.

Рекомендуется использовать Kerberos-аутентификацию, так как данный механизм является самым надежным. При NTLM-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

В этом разделе

Создание keytab-файла

Вы можете использовать одну учетную запись для аутентификации на всех узлах кластера. Для этого требуется создать keytab-файл, содержащий *имена субъекта-службы (далее также "SPN")* для каждого из этих узлов. При создании keytab-файла потребуется использовать атрибут для генерации *соли* (salt, модификатор входа хеш-функции).

Сгенерированную соль необходимо сохранить любым удобным способом для дальнейшего добавления новых SPN в keytab-файл.

Вы также можете создать отдельную учетную запись Active Directory для каждого узла кластера, для которого вы хотите настроить Kerberos-аутентификацию.

► *Чтобы создать keytab-файл, используя одну учетную запись:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте учетную запись пользователя (например, с именем `control-user`).
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) Управляющего узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <путь к файлу>\<имя файла>.keytab
```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN Управляющего узла. На экране отобразится сгенерированная соль: `Hashing password with salt "<хеш-значение>".`

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser control-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab -setupn -setpass -rawsalt "<хеш-значение соли, полученное при создании keytab-файла на шаге 3>"
```

Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL
-mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype
KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Допустим, вы получили соль `"TEST.LOCALHTTPcontrol-01.test.local"`.

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-
01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-
SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out
C:\keytabs\filename2.keytab -setupn -setpass -rawsalt
"TEST.LOCALHTTPcontrol-01.test.local"
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-
02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-
SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out
C:\keytabs\filename3.keytab -setupn -setpass -rawsalt
"TEST.LOCALHTTPcontrol-01.test.local"
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

► *Чтобы создать keytab-файл, используя отдельную учетную запись для каждого узла:*

1. На сервере контроллера домена в оснастке **Active Directory Users and Computers** создайте отдельную учетную запись пользователя для каждого узла кластера (например, учетные записи с именами `control-user`, `secondary1-user`, `secondary2-user` и т.д.).
2. Если вы хотите использовать алгоритм шифрования AES256-SHA1, то в оснастке **Active Directory Users and Computers** выполните следующие действия:
   a. Откройте свойства созданной учетной записи.
   b. На закладке **Account** установите флажок **This account supports Kerberos AES 256 bit encryption**.
3. Создайте keytab-файл для пользователя `control-user` с помощью утилиты ktpass. Для этого в командной строке выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN)
   Управляющего узла>@<realm имя домена Active Directory в верхнем
   регистре> -mapuser control-user@<realm имя домена Active Directory в
   верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass *
   -out <путь к файлу>\<имя файла>.keytab
   ```

   Утилита запросит пароль пользователя `control-user` в процессе выполнения команды.

В созданный keytab-файл будет добавлено SPN Управляющего узла.

4. Для каждого узла кластера добавьте в keytab-файл запись SPN. Для этого выполните следующую команду:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<полное доменное имя (FQDN) узла>@<realm имя домена Active Directory в верхнем регистре> -mapuser secondary1-user@<realm имя домена Active Directory в верхнем регистре> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <путь и имя ранее созданного файла>.keytab -out <путь и новое имя>.keytab
   ```

   Утилита запросит пароль пользователя `secondary1-user` в процессе выполнения команды.

Keytab-файл будет создан. Этот файл будет содержать все добавленные SPN узлов кластера.

Пример:

Например, вам нужно создать keytab-файл, содержащий SPN-имена 3 узлов: `control-01.test.local`, `secondary-01.test.local` и `secondary-02.test.local`.

Чтобы создать в папке C:\keytabs\ файл под названием `filename1.keytab`, содержащий SPN Управляющего узла, требуется выполнить команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

Для добавления еще одного SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

Для добавления третьего SPN необходимо выполнить следующую команду:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

В результате будет создан файл с именем `filename3.keytab`, содержащий все три добавленные SPN.

Настройка Kerberos-аутентификации

Для использования Kerberos-аутентификации необходимо убедиться, что в системе DNS в зонах обратного просмотра присутствует PTR-запись для полного доменного имени (FQDN) и URL (если URL отличается от FQDN) каждого узла кластера.

► *Чтобы настроить Kerberos-аутентификацию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. Выберите закладку **Kerberos**.
3. Переведите переключатель **Использовать Kerberos** в положение **Включено**.
4. Нажмите на кнопку **Загрузить**, чтобы загрузить ранее созданный keytab-файл (см. раздел "Создание keytab-файла" на стр. 270).

   Функциональность доступна только при наличии права **Изменять параметры**.

   Keytab-файл должен содержать SPN Управляющего узла и Подчиненных узлов.

   Откроется окно выбора файла.
5. Выберите keytab-файл и нажмите на кнопку **Open**.
6. Нажмите на кнопку **Сохранить**.

   Если в keytab-файле не найдено SPN Управляющего узла или SPN какого-либо из Подчиненных узлов, то для этого узла в разделе **Узлы** отображается статус *Отсутствует SPN-идентификатор для службы единого входа Kerberos*. Если в keytab-файле не найдено SPN ни одного из узлов, кнопка **Сохранить** недоступна.

Kerberos-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При отключении Kerberos-аутентификации ранее загруженный keytab-файл удаляется.

Настройка NTLM-аутентификации

Рекомендуется использовать Kerberos-аутентификацию (см. раздел "Настройка Kerberos-аутентификации" на стр. 273), так как данный механизм является самым надежным. При NTLM-аутентификации злоумышленники могут получить доступ к паролям пользователей, перехватив сетевой трафик.

► *Чтобы настроить NTLM-аутентификацию, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Вход с помощью службы единого входа**.
2. Выберите закладку **NTLM**.
3. Переведите переключатель **Использовать NTLM** в положение **Включено**.
4. В поле **IP-адрес/доменное имя контроллера домена** укажите IP-адрес или доменное имя доменного контроллера, с помощью которого будет осуществляться аутентификация.

Вы можете указать два доменных контроллера. Для добавления второго контроллера необходимо нажать на кнопку  .

5. В поле **Порт** укажите порт для подключения к доменному контроллеру.

   По умолчанию используется порт 445.

6. Нажмите на кнопку **Сохранить**.

NTLM-аутентификация будет настроена. Пользователи, прошедшие аутентификацию в Active Directory, смогут подключаться к веб-интерфейсу программы с помощью технологии единого входа. Доступ к функциональности программы будет определяться правами учетной записи программы.

При подключении с компьютеров, не входящих в домен, пользователю потребуется указать данные своей доменной учетной записи.

kaspersky

Подключение к узлам кластера по протоколу SSH

Администратор Kaspersky Secure Mail Gateway может подключиться к любому узлу кластера по протоколу SSH, чтобы работать с программой в режиме Technical Support Mode через командную строку. Для этого требуется сгенерировать ключи SSH и загрузить открытый ключ SSH через веб-интерфейс программы. После загрузки на сервер с Управляющим узлом этот ключ передается и сохраняется на всех узлах кластера.

Чтобы предотвратить несанкционированный доступ к системе, администратору требуется самостоятельно обеспечить защиту закрытого ключа SSH с помощью токена.

Вы можете добавить один или несколько открытых ключей SSH.

Добавление открытого ключа SSH

► *Чтобы загрузить открытый ключ SSH через веб-интерфейс программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Доступ SSH**.
2. Нажмите на кнопку **Добавить ключ**.

   Откроется окно **Добавьте открытый ключ SSH**.
3. В поле **Описание** введите любую информацию о загружаемом ключе SSH.
4. В поле **Данные ключа** скопируйте сгенерированный ранее открытый ключ SSH.
5. Нажмите на кнопку **Добавить**.

Открытый ключ SSH будет добавлен. Администратор Kaspersky Secure Mail Gateway сможет подключиться к любому узлу кластера при наличии соответствующего закрытого ключа SSH.

Просмотр информации об открытом ключе SSH

► *Чтобы просмотреть информацию об открытом ключе SSH, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Доступ SSH**.

   Откроется таблица открытых ключей SSH.
2. Выберите ключ, информацию о котором вы хотите просмотреть.

   Откроется окно **Просмотреть ключ SSH**.

В окне отобразится следующая информация о ключе:

- **Описание** – комментарий об открытом ключе, указанный при его добавлении в веб-интерфейс.
- **Данные ключа** – содержимое ключа.
- **Кем создан** – имя учетной записи пользователя, загрузившего ключ.
- **Когда создан** – время добавления ключа.

Удаление открытого ключа SSH

► *Чтобы удалить открытый ключ SSH, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Доступ к программе** → **Доступ SSH**.

   Откроется таблица открытых ключей SSH.
2. Выберите ключ, который вы хотите удалить.

   Откроется окно **Просмотреть ключ SSH**.
3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **ОК**.

Открытый ключ SSH будет удален.

kaspersky

Настройка параметров MTA

Kaspersky Secure Mail Gateway интегрируется в существующую почтовую инфраструктуру организации и не является самостоятельной почтовой системой. Например, Kaspersky Secure Mail Gateway не доставляет сообщения электронной почты получателям и не управляет учетными записями пользователей.

Пересылка сообщений между почтовыми серверами осуществляется с помощью агента MTA. Вы можете настроить основные и расширенные параметры MTA вручную в веб-интерфейсе программы.

В этом разделе

Настройка основных параметров MTA

Чтобы настроить основные параметры MTA, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Основные параметры**.
2. В поле **Имя домена** введите доменное имя Kaspersky Secure Mail Gateway (mydomain), которое будет использоваться для всех узлов кластера.
3. Если вы хотите, чтобы каждый узел кластера использовал собственное полное доменное имя (myhostname), переведите переключатель **Использовать FQDN узлов кластера** в положение **Включено**.
4. В поле **Имя хоста** введите полное доменное имя Kaspersky Secure Mail Gateway (myhostname).

   Поле доступно, только если опция **Использовать FQDN узлов кластера** отключена.
5. В поле **Ограничение размера сообщения (в байтах)** укажите максимальный размер пересылаемого через Kaspersky Secure Mail Gateway сообщения электронной почты (message_size_limit), включая SMTP-заголовки, в байтах.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию – 20971520 байт (20 МБ).
6. Создайте список доверенных сетей и узлов сети, которым разрешено пересылать сообщения электронной почты через Kaspersky Secure Mail Gateway (mynetworks). Для этого введите название сети в поле **Доверенные сети** и нажмите клавишу **ENTER**.

   Как правило, это внутренние сети и узлы сети вашей организации. Например, вы можете указать IP-адреса серверов Microsoft Exchange, используемых в вашей организации.

   Вы можете вводить адреса по одному или добавить сразу весь список сетей, разделенных точкой с запятой.

Если доверенные сети не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения с внутренних почтовых серверов и перенаправлять их за пределы сети вашей организации.

7. В полях **Адрес назначения сообщений** введите адрес и порт вашего пограничного шлюза (relayhost). Kaspersky Secure Mail Gateway будет перенаправлять все сообщения на этот адрес.

   Вы можете ввести IPv4-адрес (например, 192.168.0.1), доменное имя или FQDN.

   Если вы настроили маршрутизацию электронной почты для отдельных доменов (см. раздел "Домены и настройка маршрутизации электронной почты" на стр. 298), Kaspersky Secure Mail Gateway будет перенаправлять сообщения электронной почты на адреса, указанные для каждого домена.

8. Если в поле **Адрес назначения сообщений** вы указали доменное имя или FQDN, вы можете включить поиск MX-записей для указанного доменного имени. Для этого переведите переключатель **Поиск MX-записей** в положение **Включено**.

9. Нажмите на кнопку **Сохранить**.

Основные параметры MTA будут настроены.

Настройка расширенных параметров MTA

Чтобы настроить расширенные параметры MTA, выполните следующие действия:

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Расширенные параметры**.

2. В поле **Текст приветствия SMTP-сервера** введите текст, сопровождающий код 220 в SMTP-приветствии (smtpd_banner).

   Значение по умолчанию: `$myhostname ESMTP MTA`.

3. В поле **Максимум попыток соединения** задайте максимальное количество попыток соединения одного удаленного SMTP-клиента со службой SMTP-сервера в минуту (smtpd_client_connection_rate_limit).

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 0 (не ограничено).

4. В поле **Максимум одновременных попыток соединений** задайте максимальное количество одновременных попыток соединения одного удаленного SMTP-клиента с SMTP-сервером (smtpd_client_connection_count_limit).

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 50.

5. В поле **Максимум запросов на доставку сообщений** задайте максимальное количество запросов от одного удаленного SMTP-клиента к SMTP-серверу на доставку сообщений в минуту (smtpd_client_message_rate_limit), независимо от того, принимает почтовый сервер эти сообщения или нет.

   Укажите 0, если ограничения не требуются.

   Значение по умолчанию: 0 (не ограничено).

6. В поле **Максимальная длительность SMTP-сессии** задайте максимальное время, в течение которого должен быть получен запрос от удаленного SMTP-клиента и отправлен ответ SMTP-сервера (smtpd_timeout). В раскрывающемся списке рядом с полем выберите единицы измерения.

   Значение по умолчанию: 30 сек.

7. В поле **Максимальное время хранения сообщения в очереди** задайте ограничение времени хранения в очереди сообщения с временным статусом ошибки (maximal_queue_lifetime), по прошествии которого сообщение считается недоставленным. В раскрывающемся списке рядом с полем выберите единицы измерения.

   Значение по умолчанию: 3 дня.

8. В поле **Максимальное время хранения сообщения о недоставке в очереди** задайте ограничение времени хранения в очереди служебного сообщения с временным статусом ошибки (bounce_queue_lifetime), по прошествии которого сообщение считается недоставленным. В раскрывающемся списке рядом с полем выберите единицы измерения.

   Значение по умолчанию: 3 дня.

9. В поле **Адрес для скрытой копии всех сообщений** укажите необязательный адрес электронной почты для получения "blind carbon copy" всех сообщений, принятых почтовым агентом MTA (always_bcc).

10. С помощью переключателя **Проверять формат адресов по RFC 821** включите или отключите проверку адресов электронной почты в командах `SMTP MAIL FROM` и `RCPT TO` на то, что адреса заключены в угловые скобки и что эти адреса не содержат RFC 822-комментариев и фраз (strict_rfc821_envelopes).

    Такая проверка предотвращает получение сообщений от недоброкачественного программного обеспечения.

    По умолчанию проверка включена.

11. С помощью переключателя **Отключить проверку адресатов SMTP VRFY** включите или отключите команду `SMTP VRFY` (disable_vrfy_command).

    Команда `SMTP VRFY` предотвращает сбор адресов электронной почты некоторыми службами.

    По умолчанию проверка отключена.

12. В блоке параметров **Список неанонсируемых SMTP-сервером команд EHLO** установите флажки рядом с теми не чувствительными к регистру командами `EHLO`, которые ваш SMTP-сервер не будет анонсировать в ответе на `EHLO`-запрос от внешнего SMTP-клиента (smtpd_discard_ehlo_keywords).

    Значения по умолчанию: `dsn`, `etrn`.

13. Если вы хотите, чтобы Kaspersky Secure Mail Gateway отклонял запрос доставки сообщения, если для домена из заголовка `RCPT TO` отсутствуют MX- и A-записи DNS-сервера или MX-запись искажена (например, приведен адрес MX-хоста нулевой длины), переведите переключатель **Отклонять сообщения на неизвестные домены** в положение **Включено**.

    По умолчанию отклонение запросов включено.

14. В раскрывающемся списке **Отклонять сообщения на адреса получателей** выберите один из следующих режимов для SMTP-проверки адресов получателей сообщения:

    - **Не отклонять**.

      Проверка получателей не выполняется.

    - **Отклонять на адреса, не прошедшие проверку**.

Программа отклоняет сообщение, если сервер получателя недоступен или отклоняет запрос (reject_unverified_recipient).

Значение по умолчанию: **Отклонять на адреса, не прошедшие проверку**.

> SMTP-проверки адресов получателей сообщений не выполняются, если Kaspersky Secure Mail Gateway принимает сообщения с адресов доверенных узлов сети (см. раздел "Настройка основных параметров MTA" на стр. 278).
> Интенсивный почтовый трафик может увеличить нагрузку на почтовый сервер из-за отправки уведомлений о невозможности доставки сообщений.

15. Нажмите на кнопку **Сохранить**.

Расширенные параметры MTA будут настроены.

kaspersky

DKIM-подпись к исходящим сообщениям

DKIM-подпись к исходящим сообщениям – это цифровая подпись, которая добавляется к сообщениям, отправляемым с адресов электронной почты определенного домена для идентификации пользователей по имени домена организации.

Технология DomainKeys Identified Mail (DKIM) дает возможность получателю проверить, что письмо действительно было отправлено с заявленного домена. Технология DKIM предназначена для борьбы с поддельными адресами отправителей, которые часто используются в фишинговых письмах и в почтовом спаме. Вместо традиционного IP-адреса для определения отправителя сообщения используется цифровая подпись, связанная с именем домена организации. Подпись автоматически проверяется на стороне получателя. Для аутентификации отправителей используется система доменных имен (DNS), позволяющая передавать открытые ключи шифрования.

Вы можете настроить добавление DKIM-подписи к сообщениям в веб-интерфейсе Kaspersky Secure Mail Gateway. Настройка состоит из следующих этапов:

a. **Создание (см. раздел "Создание DKIM-ключа" на стр. 282) или импорт DKIM-ключа (см. раздел "Импорт DKIM-ключа из файла" на стр. 283).**
b. **Получение DNS-записи открытого DKIM-ключа (на стр. 284).**
c. **Добавление полученной DNS-записи в параметры вашего DNS-сервера (см. раздел "Добавление DKIM-ключа в параметры DNS-сервера" на стр. 284).**

В этом разделе

Создание DKIM-ключа

► *Чтобы создать DKIM-ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры → Встроенный MTA → DKIM-ключи**.
2. В верхней части рабочей области нажмите на кнопку **Создать**.

   Откроется окно **Создать новый DKIM-ключ**.
3. В поле **Название** введите имя DKIM-ключа, по которому вы сможете найти ключ при добавлении DKIM-подписи к сообщениям.
4. Нажмите на кнопку **Создать**.

Созданный вами DKIM-ключ отобразится в списке DKIM-ключей в рабочей области веб-интерфейса программы.

Просмотр информации о DKIM-ключе

► *Чтобы просмотреть информацию о DKIM-ключе, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **DKIM-ключи**.
2. Выберите DKIM-ключ, информацию о котором вы хотите просмотреть.

   Откроется окно **DKIM-ключ**.

В окне содержится следующая информация:

- **Название** – уникальное имя ключа, указанное при его создании или импорте.
- **Длина ключа** – длина ключа в битах.
- **Открытый ключ** – содержимое открытого ключа, которое можно скопировать в буфер обмена по кнопке **Копировать**.

Импорт DKIM-ключа из файла

► *Чтобы импортировать DKIM-ключ из файла, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **DKIM-ключи**.
2. В верхней части рабочей области нажмите на кнопку **Импортировать**.

   Откроется окно **Импортировать DKIM-ключ**.
3. В поле **Название** введите имя, которое вы хотите присвоить импортируемому DKIM-ключу.
4. Нажмите на кнопку **Загрузить**.

   Откроется окно выбора файлов.
5. Выберите файл DKIM-ключа, который вы хотите импортировать, и нажмите на кнопку **Open**.

   Файл должен содержать ключ RSA формата PEM длиной 2048 или 4096 бит.
6. Нажмите на кнопку **Импортировать**.

DKIM-ключ отобразится в списке DKIM-ключей в рабочей области веб-интерфейса программы.

Удаление DKIM-ключа

► *Чтобы удалить DKIM-ключ, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **DKIM-ключи**.
2. Выберите DKIM-ключ, который вы хотите удалить.

   Откроется окно **DKIM-ключ**.

3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **ОК**.

DKIM-ключ будет удален.

Получение DNS-записи открытого DKIM-ключа

► *Чтобы получить DNS-запись открытого DKIM-ключа, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Домены**.
2. Выберите домен, для которого вы хотите настроить добавление DKIM-подписи.

   Откроется окно **Изменить домен**.
3. Выберите закладку **DKIM-записи**.
4. Нажмите на кнопку **Добавить запись**.
5. Включите переключатель **Включено**.
6. В поле **Селектор** введите имя, по которому вы сможете найти DKIM-подпись.
7. В списке **DKIM-ключ** выберите DKIM-ключ, на основе которого будет добавлена DKIM-подпись к сообщениям.
8. Нажмите на кнопку **Сохранить**.

В поле **DNS-запись** отобразится DNS-запись открытого DKIM-ключа для выбранного домена.

Добавление DKIM-ключа в параметры DNS-сервера

► *Чтобы добавить открытый DKIM-ключ в параметры вашего DNS-сервера, выполните следующие действия:*

1. Авторизуйтесь на вашем DNS-сервере под учетной записью администратора.
2. Найдите страницу, содержащую информацию об обновлении DNS-записей того домена, для адресов которого вы хотите настроить добавление DKIM-подписи к исходящим сообщениям.

   Например, страница может носить название "Управление DNS", "Управление сервером имен" или "Дополнительные настройки".
3. Найдите записи формата TXT того домена, для адресов которого вы хотите настроить добавление DKIM-подписи к исходящим сообщениям.
4. В списке записей формата TXT добавьте DNS-запись открытого DKIM-ключа для определенного домена следующего содержания:

   ```
   <селектор>._domainkey.<имя домена, для которого вы хотите добавить открытый DKIM-ключ>. IN TXT ( "v=<версия DKIM>; k=rsa; s=email" "p=<DNS-запись открытого DKIM-ключа>")
   ```

Пример DNS-записи открытого DKIM-ключа:

```
sel1._domainkey.test.example.com.    IN          TXT       ( "v=DKIM1;
```

```
k=rsa; s=email; "

"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArqGgYtLwpVAFRDf+YfRK0aB5Qb
ne2xMAEye/aH4fLf7cOuOcWz/x5f33uxSpL8YwPgEXPoFogKWTFCqMUUBreHx1mbfgBn+uGYv
lxJEXyFFmiMKHO0yTJntPrWxsCnF10ZSf5lBL/olqmgCTgkpBG11PcvCJq0bdEyWQ50avMCfg
3zoean8CsiJUb91TWIy08T8HoW0huyQ3"

"W82jMhAYvO8FMgI1rbwaH7z3tlQxnGqc49+lRpz7T+p1Tl6Bs2iU8h2m1mIupIsNHF4Q+UtG
Nl9jaajhyz+NMmjLVTlaZvpbS3xODSBnZdpAXywUa4hfQsto1cHSAwEWsk90IQ/HHwIDAQAB"
)
```

> Подробнее о назначении параметров DNS-записи открытого DKIM-ключа см. в документе RFC 5617.

5. Сохраните изменения.

> Синтаксис примера DNS-записи приведен для добавления в параметры DNS-сервера BIND. Синтаксис DNS-записи, добавляемой в параметры других DNS-серверов, может незначительно отличаться от приведенного примера.

kaspersky

Использование протокола TLS в работе Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway может обрабатывать сообщения электронной почты, которые передаются по шифрованному каналу в рамках сеанса с использованием протокола TLS.

Сеанс с использованием протокола TLS (далее также TLS-сеанс) – это последовательность следующих событий:

1. Сервер, с которого отправляются сообщения электронной почты (*Клиент*), устанавливает соединение с сервером, на который отправляются сообщения электронной почты (*Сервер*).
2. Серверы начинают взаимодействие по протоколу SMTP.
3. Клиент с помощью команды `STARTTLS` предлагает Серверу использовать TLS в рамках SMTP-взаимодействия.
4. Если Сервер может использовать TLS, он отвечает командой `Ready to start TLS` и отправляет Клиенту сертификат Сервера.
5. Клиент принимает сертификат и, если для него (Клиента) настроены необходимые параметры, проверяет подлинность сертификата Сервера.
6. Клиент и Сервер включают режим шифрования данных.
7. Серверы выполняют обмен данными.
8. Сеанс заканчивается.

Вы можете настроить режим TLS-безопасности (см. раздел "Настройка TLS-безопасности для приема и отправки сообщений" на стр. 287) для ситуаций, когда Kaspersky Secure Mail Gateway принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент).

Некоторые почтовые сервера используют для обмена сообщениями электронной почты в интернете незащищенные каналы. Настройка принудительного TLS-шифрования в программе приведет к тому, что обмен сообщениями с этими серверами станет невозможен. Поэтому рекомендуется с осторожностью использовать следующие параметры TLS-безопасности:

- **Параметры TLS для приема сообщений** → **Режим TLS-безопасности сервера** = **Требовать TLS-шифрование**;
- **Параметры TLS для отправки сообщений** → **Режим TLS-безопасности клиента** = **Требовать TLS-шифрование и не проверять сертификат** или **Требовать TLS-шифрование и проверять сертификат**.

По умолчанию программа проверяет возможность TLS-шифрования, но не прерывает соединение, если шифрование недоступно. Это позволяет обеспечить обмен данными со всеми серверами, но не гарантирует защиту каналов. Сообщения электронной почты, передаваемые по незашифрованным каналам, могут быть просмотрены, подделаны или изменены злоумышленниками.

Чтобы обеспечить подлинность и конфиденциальность передаваемых сообщений, рекомендуется настроить S/MIME в параметрах почтового клиента, используемого в организации.

Если же для безопасности передачи данных вы выбрали использование TLS-шифрования в параметрах программы, то вам потребуется наличие сертификата безопасности (см. раздел "Работа с TLS-

сертификатами" на стр. 288) (далее также "TLS-сертификат"). Вы можете использовать сертификат по умолчанию, автоматически созданный программой, или добавить свой сертификат.

В этом разделе

Настройка TLS-безопасности для приема и отправки сообщений

► *Чтобы настроить режим TLS-безопасности для приема и отправки сообщений, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. В блоке параметров **Параметры TLS для приема сообщений** в раскрывающемся списке **Режим TLS-безопасности сервера** выберите один из следующих режимов TLS-шифрования соединения между Kaspersky Secure Mail Gateway и сервером, отправляющим сообщения электронной почты:
   - **Не использовать TLS-шифрование**, если вы не хотите использовать TLS-шифрование соединения с сервером, отправляющим сообщения электронной почты.

     В этом случае Kaspersky Secure Mail Gateway принимает все сообщения в незашифрованном виде.
   - **Предлагать TLS-шифрование**, если вы хотите, чтобы Kaspersky Secure Mail Gateway (Сервер) предлагал серверу, отправляющему сообщения электронной почты (Клиент), использовать TLS-шифрование соединения.

     В этом случае Kaspersky Secure Mail Gateway отправляет Клиенту список поддерживаемых SMTP-команд, в том числе и `STARTTLS`, но принимает сообщения независимо от ответа Клиента.
   - **Требовать TLS-шифрование**, если вы хотите, чтобы соединение Kaspersky Secure Mail Gateway (Сервер) с сервером, отправляющим сообщения электронной почты (Клиент), было прервано при невозможности использовать TLS-шифрование.

     В этом случае Kaspersky Secure Mail Gateway отправляет Клиенту список поддерживаемых SMTP-команд, в том числе и `STARTTLS`. Если Клиент не отвечает командой `STARTTLS`, то соединение обрывается. Если же Клиент отправляет Серверу команду `STARTTLS`, то Kaspersky Secure Mail Gateway отвечает командой `Ready to start TLS` и отправляет Клиенту сертификат сервера. После того, как Клиент проверил подлинность сертификата Сервера, устанавливается зашифрованное TLS-соединение.

   По умолчанию установлен режим **Предлагать TLS-шифрование**.
3. В раскрывающемся списке **Запрос клиентского TLS-сертификата** выберите один из следующих вариантов (недоступно для режима **Не использовать TLS-шифрование**):
   - **Не запрашивать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway не запрашивал TLS-сертификат клиента.

- **Запрашивать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway запрашивал TLS-сертификат клиента, но мог пересылать сообщения независимо от результата проверки сертификата.
- **Требовать**, если вы хотите, чтобы Kaspersky Secure Mail Gateway требовал TLS-сертификат клиента и не пересылал сообщения, если клиентский TLS-сертификат не прошел проверку подлинности.

> Устанавливайте режим **Запрашивать** или **Требовать** только если вы уверены, что клиенты, которых поддерживает ваш почтовый сервер, могут предоставить верифицируемый TLS-сертификат.

> Для корректной работы режима **Требовать** должен быть выбран режим TLS-шифрования сервера **Требовать TLS-шифрование**.

По умолчанию установлено значение **Не запрашивать**.

4. В блоке параметров **Параметры TLS для отправки сообщений** в раскрывающемся списке **Режим TLS-безопасности клиента** выберите один из следующих режимов TLS-шифрования соединения между Kaspersky Secure Mail Gateway и сервером, принимающим сообщения электронной почты:
   - **Не использовать TLS-шифрование**, если вы не хотите использовать TLS-шифрование соединения с сервером, принимающим сообщения электронной почты.

     В этом случае Kaspersky Secure Mail Gateway перенаправляет все сообщения в незашифрованном виде.
   - **Проверять возможность TLS-шифрования**, если вы хотите, чтобы Kaspersky Secure Mail Gateway пытался установить TLS-сессию с принимающим почтовым сервером и, если принимающий сервер не поддерживает TLS, перенаправлял сообщения в незашифрованном виде.
   - **Требовать TLS-шифрование и не проверять сертификат**, если вы хотите, чтобы Kaspersky Secure Mail Gateway перенаправлял сообщения только в случае, если принимающий почтовый сервер поддерживает TLS, независимо от результатов проверки подлинности TLS-сертификата.
   - **Требовать TLS-шифрование и проверять сертификат**, если вы хотите, чтобы Kaspersky Secure Mail Gateway перенаправлял сообщения только в случае, если принимающий почтовый сервер поддерживает TLS и TLS-сертификат прошел проверку подлинности.

     Kaspersky Secure Mail Gateway не перенаправляет сообщения при нарушении этих условий.

   По умолчанию установлен режим **Проверять возможность TLS-шифрования**.
5. Нажмите на кнопку **Применить**.

Режимы TLS-безопасности для приема и отправки сообщений будут настроены.

Работа с TLS-сертификатами

Для обработки сообщений, передаваемых в рамках зашифрованных TLS-соединений, требуется наличие TLS-сертификата. При создании кластера программа автоматически создает самоподписанный сертификат и использует его в качестве активного. Этот сертификат отображается в таблице TLS-сертификатов под именем **Default Cert**.

Если вы не хотите использовать сертификат, созданный по умолчанию, вы можете добавить один или несколько TLS-сертификатов, а затем назначить один из добавленных сертификатов активным (см. раздел "Назначение сертификата активным" на стр. 296). Остальные сертификаты будут отображаться в таблице с выключенным переключателем. Вы можете в любой момент назначить активным другой сертификат.

Вы можете использовать сертификаты следующих типов:

- Самоподписанный сертификат (см. раздел "Добавление самоподписанного сертификата" на стр. 289).
- Сертификат на основе CSR (см. раздел "Добавление сертификата на основе CSR" на стр. 290).
- Сертификат в формате PFX (см. раздел "Добавление сертификата в формате PFX" на стр. 292).

Сравнительные характеристики поддерживаемых в программе типов сертификатов приведены в таблице ниже.

Таблица 22. Сравнительные характеристики поддерживаемых типов сертификатов

Характеристика	Самоподписанный	На основе CSR	В формате PFX
Необходимость использовать центр сертификации	Нет	Да	Да
Хранение закрытого ключа сертификата вне кластера	Нет	Нет	Да
Возможность вручную настроить параметры сертификата	Доступно заполнение только некоторых полей	Доступно заполнение только некоторых полей	Да

В этом разделе

Добавление самоподписанного сертификата

► *Чтобы добавить самоподписанный сертификат, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. Нажмите на кнопку **Создать сертификат**.

   Откроется окно **Создать сертификат**.
3. Выберите вариант **Создать самоподписанный сертификат**.

4. В поле **Организация** введите название организации.
5. В поле **Общее имя** введите доменное имя сервера, для которого создается сертификат.
6. Нажмите на кнопку **Создать**.

Сертификат будет добавлен и отобразится в таблице TLS-сертификатов.

Добавление сертификата на основе CSR

Добавление сертификата на основе CSR состоит из следующих этапов.

a. **Создание файла запроса в веб-интерфейсе программы (см. раздел "Создание файла запроса" на стр. 290)**
b. **Формирование сертификата на основе файла запроса в центре сертификации**
c. **Загрузка сформированного сертификата в веб-интерфейсе программы (см. раздел "Загрузка сертификата в веб-интерфейсе программы" на стр. 292)**

   В программе доступна загрузка отдельных сертификатов в виде файлов с расширениями .pem, .der, .cer, .crt, а также файлов-контейнеров PKCS#7 с расширением .p7b, содержащих цепочку сертификатов.

В этом разделе

Создание файла запроса

► *Чтобы создать файл запроса, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. Нажмите на кнопку **Создать сертификат**.

   Откроется окно **Создать сертификат**.
3. Выберите вариант **Создать CSR-запрос**.
4. В поле **Организация** введите название организации.
5. В поле **Общее имя** введите доменное имя сервера, для которого создается сертификат.
6. В поле **FQDN** введите список полных доменных имен всех узлов кластера через точку с запятой.

   Если удаленные MTA взаимодействуют напрямую с узлами кластера (для кластера не используется общее виртуальное балансируемое DNS-имя), то указание FQDN всех узлов кластера необходимо для успешной верификации сертификата. Указанные FQDN будут внесены в расширенный атрибут сертификата Subject Alt name. В случае изменения состава кластера или изменения FQDN узлов кластера может потребоваться пересоздание сертификата с актуальным списком FQDN. Обычно верификация сертификата не является обязательной для шифрования почтового трафика.

7. Нажмите на кнопку **Создать**.

   Запись о запросе CSR отобразится в таблице TLS-сертификатов. Откроется окно **Просмотреть сертификат**.

8. Нажмите на кнопку **Скачать CSR-файл**.

Файл запроса будет сохранен в папку загрузки браузера. Используйте этот файл запроса для формирования сертификата в центре сертификации.

Формирование сертификата в центре сертификации

Инструкция приведена для центра сертификации Microsoft Enterprise Certification Authority, развернутом на сервере Windows Server 2016.

Рекомендуется использовать браузер Internet Explorer®. В других браузерах могут некорректно отображаться некоторые страницы центра сертификации Microsoft Enterprise Certification Authority.

► *Чтобы сформировать сертификат на основе CSR, выполните следующие действия:*

1. Откройте созданный ранее файл запроса (см. раздел "Создание файла запроса" на стр. 290) в любом текстовом редакторе и скопируйте его содержимое в буфер обмена.
2. Откройте в браузере страницу вашего центра сертификации: `https://<адрес сервера>/certsrv`.
3. Выберите **Request a certificate**.

   Откроется страница **Request a Certificate**.

4. Выберите **advanced certificate request**.

   Откроется страница **Advanced Certificate Request**.

5. Выберите **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

   Откроется страница **Submit a Certificate Request or Renewal Request**.

6. В поле **Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)** вставьте содержимое файла запроса, скопированное на шаге 1.
7. В раскрывающемся списке **Certificate Template** выберите один из следующих вариантов:
   - шаблон с расширением **Server Authentication**, если вы хотите использовать сертификат в качестве серверного.
   - шаблон с расширением **Client Authentication**, если вы хотите использовать сертификат в качестве клиентского.
   - шаблон с расширениями **Server Authentication** и **Client Authentication**, если вы хотите использовать сертификат в качестве серверного и клиентского.
8. Нажмите на кнопку **Submit**.

   Откроется страница **Certificate Issued**.

9. Выполните следующие действия:
   a. Выберите кодировку файла сертификата.

Программа поддерживает работу с сертификатами в кодировке DER и Base64.

b. Выберите формат сертификата:

- Если вы хотите скачать файл конечного сертификата с расширением .cer, не содержащий промежуточных сертификатов, выберите **Download certificate**.
- Если вы хотите скачать полную цепочку сертификатов в формате PKCS#7-контейнера с расширением .p7b, выберите **Download certificate chain**.

> Рекомендуется скачать полную цепочку сертификатов, чтобы избежать проблем с проверкой промежуточных центров сертификации.

Сертификат будет сформирован и сохранен на вашем компьютере в папке загрузки браузера.

Загрузка сертификата в веб-интерфейсе программы

► *Чтобы загрузить сертификат на основе CSR в веб-интерфейсе программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры → Встроенный MTA → TLS-шифрование**.
2. В таблице TLS-сертификатов выберите запись о созданном ранее файле запроса CSR (см. раздел "Создание файла запроса" на стр. 290).

   Откроется окно **Просмотреть сертификат**.
3. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файлов.
4. Выберите файл сертификата, сформированный в центре сертификации, и нажмите на кнопку **Open**.
5. Нажмите на кнопку **Загрузите подписанный сертификат**.

   В окне **Просмотреть сертификат** отобразится отпечаток сертификата и дата его истечения.

Сертификат будет загружен. В таблице TLS-сертификатов тип сертификата изменится с **Запрос CSR** на **На основе CSR**.

Добавление сертификата в формате PFX

Добавление сертификата в формате PFX состоит из следующих этапов.

a. **Формирование сертификата в центре сертификации**

   Сертификат с закрытым ключом формируется в формате PKCS#12-контейнера и сохраняется в хранилище сертификатов текущего пользователя.

b. **Экспорт сертификата в файл (на стр. 294)**

   После формирования сертификата необходимо экспортировать его вместе с закрытым ключом в файл с расширением .p12 или .pfx.

c. **Загрузка сертификата в веб-интерфейсе программы (на стр. 295)**

kaspersky

В этом разделе

Формирование сертификата в центре сертификации

Инструкция приведена для центра сертификации Microsoft Certification Authority, развернутом на сервере Windows Server 2016.

Рекомендуется использовать браузер Internet Explorer. В других браузерах могут некорректно отображаться некоторые страницы центра сертификации Microsoft Certification Authority.

► *Чтобы сформировать PFX-сертификат с закрытым ключом, выполните следующие действия:*

1. Откройте в браузере страницу вашего центра сертификации: `https://<адрес сервера>/certsrv`.
2. Выберите **Request a certificate**.

   Откроется страница **Request a certificate**.
3. Выберите **advanced certificate request**.

   Откроется страница **Advanced Certificate Request**.
4. Выберите **Create and submit a request to this CA**.

   Откроется страница **Advanced Certificate Request**.
5. В раскрывающемся списке **Certificate Template** выберите один из следующих вариантов:
   - шаблон с расширением **Server Authentication**, если вы хотите использовать сертификат в качестве серверного.
   - шаблон с расширением **Client Authentication**, если вы хотите использовать сертификат в качестве клиентского.
   - шаблон с расширениями **Server Authentication** и **Client Authentication**, если вы хотите использовать сертификат в качестве серверного и клиентского.
6. В блоке параметров **Identifying Information For Offline Template** заполните информацию о вашей организации.

   Поле **Name** является обязательным.
7. В блоке параметров **Key Options** выполните следующие действия:
   a. Выберите вариант **Create new key set**.
   b. В поле **Key Size** введите значение 2048.
   c. Выберите вариант **Automatic key container name**.

d. Установите флажок **Mark keys as exportable**.

8. В блоке параметров **Additional Options** убедитесь, что флажок **Save request** снят.
9. Нажмите на кнопку **Submit**.

   Откроется страница **Certificate Issued**.

10. Выберите **Install this certificate**.

Сертификат с закрытым ключом будет сформирован и сохранен в хранилище сертификатов вашей учетной записи.

Экспорт сертификата в файл

► *Чтобы экспортировать сертификат с закрытым ключом в файл, выполните следующие действия:*

1. Откройте консоль управления Microsoft (MMC).
2. Выберите **File** → **Add/Remove Snap-in**.

   Откроется окно **Add or Remove Snap-ins**.

3. Выберите оснастку **Certificates** и нажмите кнопку **Add**.

   Откроется окно **Certificates Snap-in**.

4. Выберите **My user account** и нажмите **Finish**.
5. В окне **Add/Remove Snap-ins** нажмите **OK**.
6. В дереве консоли выберите **Certificates – Current User** → **Personal** → **Certificates**.
7. В рабочей области выберите сертификат, сформированный ранее, и двойным нажатием откройте его свойства.
8. Выберите закладку **Details**.
9. Нажмите кнопку **Copy to File**.

   Запустится мастер экспорта сертификата.

10. В окне **Export Private Key** выберите вариант **Yes, export the private key**.
11. В окне **Export File Format** выполните следующие действия:
    a. Выберите вариант **Personal Information Exchange – PKCS #12 (.PFX)**.
    b. Установите флажок **Include all certificates in the certification path if possible**.
12. В окне **Security** выполните следующие действия:
    a. Установите флажок **Password**.
    b. В поле ввода под флажком задайте пароль для защиты сертификата.
    c. В поле **Confirm password** повторите пароль.
13. В окне **File to Export** выполните следующие действия:
    a. Нажмите на кнопку **Browse**.
    b. Откроется окно **Save as**.
    c. Выберите путь для сохранения файла сертификата на вашем компьютере.
    d. Введите имя файла и нажмите на кнопку **Save**.

14. В окне **Completing the Certificate Export Wizard** нажмите на кнопку **Finish**.

Сертификат с закрытым ключом будет экспортирован в файл. Файл будет сохранен на вашем компьютере по указанному пути.

Загрузка сертификата в веб-интерфейсе программы

► *Чтобы загрузить сертификат с закрытым ключом в веб-интерфейсе программы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. Нажмите на кнопку **Создать сертификат**.

   Откроется окно **Создать сертификат**.
3. Выберите вариант **Импортировать сертификат в формате PFX**.
4. Нажмите на кнопку **Обзор**.

   Откроется окно выбора файла.
5. Выберите файл, в который вы экспортировали сертификат с закрытым ключом (см. раздел "Экспорт сертификата в файл" на стр. 294), и нажмите на кнопку **Open**.

   Имя файла сертификата отобразится в поле ввода слева от кнопки **Загрузить**.
6. В поле **Пароль PFX** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.
7. Нажмите на кнопку **Создать**.

Сертификат будет добавлен и отобразится в таблице TLS-сертификатов.

Просмотр информации о сертификате

► *Чтобы просмотреть информацию о сертификате, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. В таблице TLS-сертификатов выберите сертификат, информацию о котором вы хотите просмотреть.

   Откроется окно **Просмотреть сертификат**.

В окне содержится следующая информация о сертификате:

- **Субъект** – общее имя (CN, Common Name) и название организации владельца сертификата (O, Organization).
- **Дата истечения** – дата и время окончания срока действия сертификата.
- **Тип** – один из следующих типов сертификата:
  - **Самоподписанный**.
  - **На основе CSR**.
  - **В формате PFX**.

- **Отпечаток сертификата (SHA256)** – отпечаток сертификата SHA256.

Назначение сертификата активным

Вы можете использовать добавленный TLS-сертификат в качестве активного серверного или клиентского сертификата. Если вы используете TLS-шифрование, то наличие активного серверного сертификата обязательно. Активный клиентский сертификат является опциональным даже при включенном режиме TLS-безопасности клиента.

► *Чтобы назначить сертификат активным, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. Чтобы назначить TLS-сертификат, который будет использоваться при обработке входящих подключений по протоколу SMTP, в качестве активного серверного сертификата, в строке с нужным сертификатом включите переключатель в графе **Использовать как серверный сертификат**.
3. Чтобы назначить TLS-сертификат, который будет использоваться при обработке исходящих подключений по протоколу SMTP, в качестве активного клиентского сертификата, в строке с нужным сертификатом включите переключатель в графе **Использовать как клиентский сертификат**.

Сертификат будет назначен активным.

► *Чтобы отключить использование сертификата в качестве активного, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. Если вы хотите отключить использование серверного сертификата в качестве активного, назначьте другой сертификат активным с помощью переключателя в графе **Использовать как серверный сертификат**.

   Ранее использованный серверный сертификат автоматически перестанет быть активным.
3. Если вы хотите отключить использование клиентского сертификата в качестве активного, в строке с этим сертификатом отключите переключатель в графе **Использовать как клиентский сертификат**.

Сертификат перестанет использоваться в качестве активного.

Скачивание сертификата

► *Чтобы скачать сертификат, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. В таблице TLS-сертификатов выберите сертификат, который вы хотите скачать.

   Откроется окно **Просмотреть сертификат**.
3. Нажмите на одну из следующих кнопок в зависимости от требуемого формата сертификата:
   - **Скачать P7B-цепочку** – цепочка сертификатов в формате .p7b.
   - **Скачать CRT-файл** – конечный сертификат в формате .crt.

Сертификат или цепочка сертификатов будут сохранены в папку загрузки браузера.

Удаление сертификата

► *Чтобы удалить сертификат, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **TLS-шифрование**.
2. В таблице TLS-сертификатов выберите сертификат, который вы хотите удалить.

   Откроется окно **Просмотреть сертификат**.

   > Удаление активного сертификата недоступно.

3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Сертификат будет удален.

kaspersky

Домены и настройка маршрутизации электронной почты

Этот раздел содержит информацию о том, как добавлять домены и адреса электронной почты в транспортную таблицу, настраивать маршрутизацию электронной почты для этих доменов, удалять домены из списка, настраивать режимы TLS-безопасности для исходящих сообщений электронной почты и добавлять DKIM-подпись к сообщениям.

Kaspersky Secure Mail Gateway по умолчанию использует параметры вашего DNS-сервера для маршрутизации электронной почты. Вы можете настроить маршрутизацию электронной почты вручную. Для этого необходимо создать транспортную таблицу. В нее нужно ввести имена доменов, для которых предназначены сообщения электронной почты, ввести IP-адреса, FQDN-имена или имена доменов, на которые Kaspersky Secure Mail Gateway будет перенаправлять сообщения, предназначенные для этих доменов.

Пример:

Если вы хотите, чтобы сообщения, предназначенные для домена example.com, перенаправлялись на адрес 192.168.0.1:25, вам нужно выполнить следующие действия:

1. Добавить домен example.com в транспортную таблицу.
2. Указать IP-адрес 192.168.0.1 и номер порта 25 для маршрутизации сообщений, предназначенных для домена example.com.

В этом разделе также описана настройка маршрутизации электронной почты для локальных доменов (relay_domains).

Локальные домены (relay_domains) – домены вашей организации, для которых Kaspersky Secure Mail Gateway будет принимать сообщения электронной почты извне. Kaspersky Secure Mail Gateway будет принимать сообщения только для указанных вами доменов. Сообщения, предназначенные для получения другими доменами, будут отклонены.

Если локальные домены не указаны, Kaspersky Secure Mail Gateway не будет принимать сообщения для ваших внутренних почтовых серверов.

В этом разделе

kaspersky

Просмотр транспортной таблицы для доменов

► *Чтобы просмотреть транспортную таблицу для доменов,*

в окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Домены**.

В таблице отображается следующая информация о записях в транспортной таблице:

- **Запись** – имя домена, поддомена или адрес электронной почты, для которого настроена маршрутизация.
- **Тип домена** – тип записи в транспортной таблице (домен, поддомен или адрес электронной почты).
- **Локальный домен** – переключатель, позволяющий регулировать, является ли запись в транспортной таблице локальным доменом (не отображается для записи типа **Адрес эл.почты**).
- **Протокол** – протокол передачи электронной почты, используемый при маршрутизации. Доступны протоколы SMTP и LMTP, по умолчанию используется протокол SMTP.
- **Адрес назначения** – IP-адрес, имя сервера или доменное имя, на которое настроена маршрутизация почты.
- **Порт** – порт соединения с сервером, на который настроена маршрутизация почты.
- **Режим TLS-безопасности** – режим TLS-шифрования соединения, используемый для этого домена или поддомена (не отображается для записи типа **Адрес эл.почты**), который будет использоваться при исходящих сообщениях на этот домен или поддомен.
- **DKIM-записи** – DNS-запись открытого DKIM-ключа, необходимая для настройки DKIM-подписи к сообщениям.

Добавление записи в транспортную таблицу и настройка маршрутизации электронной почты (transport_map)

► *Чтобы добавить запись в транспортную таблицу и настроить маршрутизацию электронной почты, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Домены**.
2. Нажмите на кнопку **Добавить домен**.

   Откроется окно создания записи.
3. В раскрывающемся списке **Тип записи** выберите один из следующих типов записи:
   - **Домен**.
   - **Поддомены**.
   - **Адрес эл.почты**.
4. В поле ниже введите имя домена, имя поддомена в формате FQDN или адрес электронной почты.
5. Включите переключатель **Локальный домен**, если вы хотите добавить локальный домен.
6. Включите переключатель **Маршрутиризация**, если вы хотите настроить маршрутизацию почты для добавляемой записи.

7. В раскрывающемся списке **Протокол** выберите один из протоколов передачи электронной почты:
   - **SMTP**.
   - **LMTP**.
8. В поле **Хост** введите IP-адрес, FQDN имя сервера или имя домена, на который вы хотите настроить маршрутизацию почты.

   Вы можете ввести IPv4-адрес (например, 192.168.0.1), доменное имя или FQDN.
9. В поле **Порт** введите порт подключения к серверу, на который вы хотите настроить маршрутизацию почты.
10. Включите или отключите поиск MX-записей с помощью переключателя **Поиск MX-записей DNS**.
11. Если вы добавляете домен или поддомены домена, в блоке параметров **Режим TLS-шифрования для исходящих сообщений** выберите один из следующих вариантов:
    - **Использовать режим <режим, установленный в разделе TLS-шифрование>**, если для исходящих сообщений на этот домен или поддомен вы хотите использовать режим TLS-шифрования соединения, установленный для всех исходящих сообщений почтового сервера.
    - **Изменить режим TLS-шифрования для этого домена**, если вы хотите настроить другой режим TLS-шифрования соединения для исходящих сообщений на этот домен или поддомен.
12. Если вы выбрали изменение режима TLS-шифрования для этого домена или поддомена, в раскрывающемся списке ниже выберите режим TLS-шифрования соединения, который вы хотите установить:
    - **Не использовать TLS-шифрование**.
    - **Проверять возможность TLS-шифрования**.
    - **Требовать TLS-шифрование и не проверять сертификат**.
    - **Требовать TLS-шифрование и проверять сертификат**.

    По умолчанию установлен режим **Не использовать TLS-шифрование**.
13. Нажмите на кнопку **Сохранить**.

Добавленная запись отобразится в транспортной таблице.

Изменение маршрутизации электронной почты

► *Чтобы изменить маршрутизацию электронной почты, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Домены**.
2. В транспортной таблице выберите запись, для которой вы хотите изменить параметры маршрутизации электронной почты.

   Откроется окно **Изменить домен**.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Сохранить**.

Маршрутизация электронной почты для этой записи транспортной таблицы будет изменена.

kaspersky

Удаление записи из транспортной таблицы

► *Чтобы удалить запись из транспортной таблицы, выполните следующие действия:*

1. В окне веб-интерфейса программы выберите раздел **Параметры** → **Встроенный MTA** → **Домены**.
2. В транспортной таблице выберите запись, которую вы хотите удалить.

   Откроется окно **Изменить домен**.
3. Нажмите на кнопку **Удалить**.
4. В окне подтверждения нажмите на кнопку **Да**.

Запись будет удалена из транспортной таблицы.

kaspersky

Публикация событий программы в SIEM-систему

Kaspersky Secure Mail Gateway может публиковать события, происходящие во время работы программы, в *SIEM-систему*, которая уже используется в вашей организации, по протоколу Syslog.

Информация о каждом событии программы передается как отдельное syslog-сообщение формата CEF (см. раздел "Содержание и свойства syslog-сообщений в формате CEF" на стр. 306) (далее также "CEF-сообщение").

CEF-сообщение с информацией о событии передается сразу после появления события. Исключение – классы событий группы ScanLogic, все CEF-сообщения этих классов передаются после обработки сообщений электронной почты модулем ScanLogic.

По умолчанию экспорт CEF-сообщений в программе отключен. Вы можете включить экспорт событий (см. раздел "Настройка экспорта событий в формате CEF" на стр. 302) и настроить их публикацию в SIEM-систему (см. раздел "Настройка публикации событий программы в SIEM-систему" на стр. 305).

В этом разделе

Настройка экспорта событий в формате CEF

Для включения экспорта событий в режиме Technical Support Mode требуется предварительно загрузить открытый ключ SSH в веб-интерфейсе программы (см. раздел "Добавление открытого ключа SSH" на стр. 276).

Вы можете сохранять файлы с экспортированными событиями локально на сервере, а также настроить их публикацию во внешнюю SIEM-систему (см. раздел "Настройка публикации событий программы в SIEM-систему" на стр. 305). Если вам не требуется сохранять файлы локально, пропустите шаги 5–7 из инструкции этого раздела.

Выполните инструкцию ниже на каждом узле кластера, события с которого вы хотите экспортировать в формате CEF.

► *Чтобы настроить экспорт событий в формате CEF:*

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью root, используя закрытый ключ SSH.

   Вы войдете в режим Technical Support Mode.

2. Внесите следующие изменения в файл с параметрами экспорта событий /opt/kaspersky/ksmg/share/templates/core_settings/event_logger.json.template:

   - Если вы хотите выбрать категорию (facility) для syslog, в которую будут экспортироваться события, в блоке `siemSettings` укажите одно из следующих значений параметра `facility`:
     - `Auth`.
     - `Authpriv`.
     - `Cron`.
     - `Daemon`.
     - `Ftp`.
     - `Lpr`.
     - `Mail`.
     - `News`.
     - `Syslog`.
     - `User`.
     - `Uucp`.
     - `Local0`.
     - `Local1`.
     - `Local2`.
     - `Local3`.
     - `Local4`.
     - `Local5`.
     - `Local6`.
     - `Local7`.

     Рекомендуется указать такую категорию (facility) для syslog, которая не используется другими программами на сервере.

     По умолчанию установлено значение `local2`.
   - Установите значение параметра `enabled` равным `true`.
   - Задайте уровень детализации экспорта, установив одно из следующих значений параметра `logLevel`:
     - `Error` – экспорт событий, связанных с возникновением ошибок.
     - `Info` – экспорт всех событий.

Пример:

```
"siemSettings":
  {
    "enabled": true,
    "facility": "Local2",
    "logLevel": "Info",
  }
```

3. В файле /etc/rsyslog.conf измените строку

   ```
   *.info;mail.none;authpriv.none;cron.none;local0.none;local1.none
   /var/log/messages
   ```

   на

   ```
   *.info;mail.none;authpriv.none;cron.none;local0.none;local1.none;<катег
   ория (facility), выбранная на шаге 2>.none    /var/log/messages
   ```

4. Добавьте в файл /etc/rsyslog.conf следующую строку:

   ```
   <категория (facility), выбранная на шаге 2>.* -/var/log/ksmg-cef-
   messages
   ```

5. Создайте файл /var/log/ksmg-cef-messages и настройте права доступа к нему. Для этого выполните команды:

   ```
   touch /var/log/ksmg-cef-messages
   chown root:klusers /var/log/ksmg-cef-messages
   chmod 640 /var/log/ksmg-cef-messages
   ```

6. Настройте правила ротации файлов с экспортированными событиями. Для этого добавьте в файл /etc/logrotate.d/ksmg-syslog следующие строки:

   ```
   /var/log/ksmg-cef-messages
   {
       size 500M
       rotate 10
       notifempty
       sharedscripts
       postrotate
           /usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1
   || true
       endscript
   }
   ```

7. Перезапустите службу rsyslog. Для этого выполните команду:

   ```
   service rsyslog restart
   ```

8. В веб-интерфейсе программы в разделе **Параметры** → **Журналы и события** → **События** внесите изменение в значение любого параметра и нажмите на кнопку **Сохранить**.

   Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого вы можете вернуть исходное значение измененного параметра.

Экспорт событий в формате CEF будет настроен.

Настройка публикации событий программы в SIEM-систему

Для настройки публикации событий в режиме Technical Support Mode требуется предварительно загрузить открытый ключ SSH в веб-интерфейсе программы (см. раздел "Добавление открытого ключа SSH" на стр. 276).

Перед началом настройки убедитесь, что вы включили экспорт событий в формате CEF (см. раздел "Настройка экспорта событий в формате CEF" на стр. 302).

Выполните инструкцию ниже на каждом узле кластера, события с которого вы хотите публиковать в SIEM-систему.

► *Чтобы настроить публикацию событий программы в SIEM-систему, выполните следующие действия:*

1. Подключитесь к консоли управления виртуальной машиной Kaspersky Secure Mail Gateway под учетной записью root, используя закрытый ключ SSH.

   Вы войдете в режим Technical Support Mode.

2. Укажите адрес и порт подключения к серверу с SIEM-системой. Для этого добавьте в конец файла /etc/rsyslog.conf следующие строки:

   ```
   $WorkDirectory /var/lib/rsyslog

   $ActionQueueFileName ForwardToSIEM

   $ActionQueueMaxDiskSpace 1g

   $ActionQueueSaveOnShutdown on

   $ActionQueueType LinkedList

   $ActionResumeRetryCount -1

   <категория (facility)>.* @@<IP-адрес SIEM-системы>:<порт, на котором SIEM-система принимает сообщения от Syslog по протоколу TCP>
   ```

Перед внесением изменений в файл /etc/rsyslog.conf рекомендуется сделать его резервную копию. Ошибка при редактировании файла может привести к некорректной работе системы.

3. Перезапустите службу rsyslog. Для этого выполните команду:

   ```
   service rsyslog restart
   ```

Публикация событий программы в SIEM-систему будет настроена.

Содержание и свойства syslog-сообщений в формате CEF

Информация о каждом обнаруженном событии передается как отдельное syslog-сообщение формата CEF, имеющее кодировку UTF-8.

Сообщение в формате CEF состоит из *тела сообщения* и *заголовка*. В каждом syslog-сообщении передаются следующие поля, определяемые параметрами протокола Syslog в операционной системе:

- дата и время события;
- имя хоста, на котором произошло событие;
- название программы (всегда имеет значение `Kaspersky Secure Mail Gateway`).

Поля syslog-сообщения о событии, определяемые параметрами программы, представлены в формате `<ключ>="<значение>"`. Если ключ имеет несколько значений, эти значения указываются через запятую. В качестве разделителя между ключами используется двоеточие.

Ключи, а также их значения, содержащиеся в сообщении, зависят от класса события.

Пример:

```
July 16, 2017 10:34:23 host.domain.com

CEF:0|AO Kaspersky Lab|Kaspersky Secure Mail
Gateway|2.0.0.1234|LMS_EV_SETTINGS_CHANGED|task settings
changed|severity|cn1=taskId cn1Label=TaskId cs1=taskName csLabel=TaskName
act=created/changed/deleted
```

Максимальный размер syslog-сообщения об обнаруженном событии зависит от значений параметров syslog на сервере, на котором установлен Kaspersky Secure Mail Gateway. Вы можете настроить пересылку syslog-сообщений только на один внешний syslog-сервер единовременно.

Классы событий группы Settings

В теле CEF-сообщений классов событий группы Settings допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 23. Допустимые значения полей классов событий группы Settings

Ключ	Значение
cn1	Номер задачи (из klms-control).

Ключ	Значение
cn1Label	Всегда имеет значение `TaskId`.
cs1	Имя задачи (из klms-control).
cs1Label	Всегда имеет значение `TaskName`.
duser	Пользователь, чьи параметры были изменены.
suser	Пользователь, который изменил параметры.
act	Действие, выполненное с параметрами. Допустимые значения: `created`, `changed`, `deleted`.

В каждом классе событий группы Settings допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 24. Релевантные ключи для классов событий группы Settings

Класс событий	Релевантные ключи
LMS_EV_SETTINGS_CHANGED	cn1, cn1Label, cs1, cs1Label, act
LMS_EV_ALL_SETTINGS_CHANGED	suser
LMS_EV_PERSONAL_SETTINGS_CHANGED	suser, duser

Классы событий группы Tasks

В теле CEF-сообщений классов событий группы Tasks допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 25. Допустимые значения полей классов событий группы Tasks

Ключ	Значение
deviceProcessName	Имя задачи (из klms-control).
cs1	Режим работы программы (`real time scan` / `configuration mode`).
cs1Label	Всегда имеет значение `Mode`.

В каждом классе событий группы Tasks допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 26. Релевантные ключи для классов событий группы Tasks

Класс событий	Релевантные ключи
LMS_EV_PROCESS_CRASHED	deviceProcessName
LMS_EV_RESTARTED	deviceProcessName
LMS_EV_PRODUCT_STARTED	cs1, cs1Label

Классы событий группы Backup

В теле CEF-сообщений классов событий группы Backup допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 27. Допустимые значения полей для классов событий группы Backup

Ключ	Значение
cn1	Размер сообщения.
cn1Label	Всегда имеет значение `MessageSize`.
cn2	Максимальный размер Хранилища.
cn2Label	Всегда имеет значение `MaxBackupSize`.
cn3	Количество сообщений в Хранилище.
cn3Label	Всегда имеет значение `MessageCount`.
cs1	ID сообщения в Хранилище.
cs1Label	Всегда имеет значение `MessageId`.
cnt	Количество ошибок за последние 10 минут.
act	Действие над сообщением в Хранилище (доставить / удалить).
suser	Пользователь, который выполнил действие с сообщением в Хранилище.
cs2	Статус антивирусной проверки.
cs2Label	Всегда имеет значение `AvStatus`.
cs3	Статус проверки ссылок.
cs3Label	Всегда имеет значение `MlfStatus`.
cs4	Статус проверки на спам.

Ключ	Значение
cs4Label	Всегда имеет значение `AsStatus`.
cs5	Статус проверки на фишинг.
cs5Label	Всегда имеет значение `ApStatus`.
cs6	Имя вредоносного объекта.
cs6Label	Всегда имеет значение `Threat`.
cs7	Статус контентной фильтрации.
cs7Label	Всегда имеет значение `CfStatus`.
duser	Список получателей сообщения.
reason	Описание ошибки.

В каждом классе событий группы Backup допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 28. Релевантные ключи для классов событий группы Backup

Класс событий	Релевантные ключи
LMS_EV_BACKUP_ADD_ERROR	cs1, cs1Label, cnt
LMS_EV_BACKUP_ROTATE_ERROR	reason, cnt
LMS_EV_BACKUP_MESSAGE_RESTORE	cs1, cs1Label, act, suser, cs2, cs2Label, cs3, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, duser

Классы событий группы License

В теле CEF-сообщений классов событий группы License допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 29. Допустимые значения полей классов событий группы License

Ключ	Значение
cs1	Серийный номер лицензии.
cs1Label	Всегда имеет значение `LicenseID`.
cs2	Режим работы Kaspersky Secure Mail Gateway в соответствии с лицензией.
cs2Label	Всегда имеет значение `FunctionalityLevel`.

Ключ	Значение
cs3	Тип лицензии.
cs3Label	Всегда имеет значение `KeyType`.
cn1	Количество дней до истечения срока действия лицензии.
cn1Label	Всегда имеет значение `DaysLeft`.
reason	Описание ошибки.
deviceCustomDate1	Дата истечения срока действия лицензии.
deviceCustomDate1Label	Всегда имеет значение `ExpirationDate`.

В каждом классе событий группы License допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 30. Релевантные ключи для классов событий группы License

Класс событий	Релевантные ключи
LMS_EV_LICENSE_OK	cs1, cs1Label, cs2, cs2Label
LMS_EV_LICENSE_INVALID	cs1, cs1Label, reason
LMS_EV_NO_LICENSE	Нет значения
LMS_EV_LICENSE_BLACKLISTED	cs1, cs1Label
LMS_EV_LICENSE_TRIAL_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_EXPIRED	cs1, cs1Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_LICENSE_ERROR	reason
LMS_EV_LICENSE_INSTALLED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label
LMS_EV_LICENSE_UPDATED	cs1, cs1Label, cs2, cs2Label, cs3, cs3Label, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_GRACE_PERIOD	cs1, cs1Label, cn1, cn1Label
LMS_EV_LICENSE_REVOKED	cs1, cs1Label
LMS_EV_LICENSE_EXPIRES_SOON	cs1, cs1Label, cn1, cn1Label

kaspersky

Классы событий группы Rules

В теле CEF-сообщений классов событий группы Rules допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 31. Допустимые значения полей классов событий группы Rules

Ключ	Значение
cs1	Имя правила.
cs1Label	Всегда имеет значение `RuleName`.
cn1	ID правила.
cn1Label	Всегда имеет значение `RuleId`.
act	Действие с правилом (`created` / `settings changed` / `deleted` / `priotity changed`).

В каждом классе событий группы Rules допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 32. Релевантные ключи для классов событий группы Rules

Класс событий	Релевантные ключи
LMS_EV_RULE_CHANGED	cs1, cs1Label, cn1, cn1Label, act
LMS_EV_ALL_RULES_IMPORTED	Нет значения

Классы событий группы Quarantine

В теле CEF-сообщений классов событий группы Quarantine допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 33. Допустимые значения полей классов событий группы Quarantine

Ключ	Значение
cs1	ID сообщения.
cs1Label	Всегда имеет значение `MessageId`.
cs2	Список правил через запятую.
cs2Label	Всегда имеет значение `Rules`.
cs3	Учетная запись, под которой было выполнено действие над сообщением.
cs3Label	Всегда имеет значение `Account`.

Ключ	Значение
src	IP-адрес, с которого получено сообщение.
duser	Список получателей сообщения.
suser	Отправитель сообщения.
act	Действие над сообщением (`proceed` / `delete`).

В каждом классе событий группы Quarantine допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 34. Релевантные ключи для классов событий группы Quarantine

Класс событий	Релевантные ключи
LMS_EV_ASP_QUARANTINE	cs1, cs1Label, src, suser, cs3, cs3Label, act
LMS_EV_KATA_QUARANTINE	cs1, cs1Label, cs2, cs2Label, suser, duser, act, cs3, cs3Label

Классы событий группы Update

В теле CEF-сообщений классов событий группы Update допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 35. Допустимые значения полей классов событий группы Update

Ключ	Значение
reason	Причина возникновения события.
cn1	Количество дней.
cn1Label	Всегда имеет значение `Days`.
cn2	Количество часов.
cn2Label	Всегда имеет значение `Hours`.
cnt	Количество записей в базах.
deviceCustomDate1	Дата публикации баз.
deviceCustomDate1Label	Всегда имеет значение `PublishingTime`.
deviceCustomDate2	Дата публикации индекса.
deviceCustomDate2Label	Всегда имеет значение `IndexPublishingTime`.

В каждом классе событий группы Update допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 36. Релевантные ключи для классов событий группы Update

Класс событий	Релевантные ключи
LMS_EV_ANTIVIRUS_BASES_UPDATED	Нет значения
LMS_EV_ANTISPAM_BASES_UPDATED	Нет значения
LMS_EV_ANTIPHISHING_BASES_UPDATED	Нет значения
LMS_EV_BASES_NOTHING_TO_UPDATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIPHISHING_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTISPAM_BASES_UP_TO_DATE	Нет значения
LMS_EV_ANTIVIRUS_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OUT_OF_DATE	cn1, cn1Label
LMS_EV_ANTISPAM_BASES_OUT_OF_DATE	cn2, cn2Label
LMS_EV_ANTIVIRUS_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIPHISHING_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTISPAM_BASES_OBSOLETED	cn1, cn1Label
LMS_EV_ANTIVIRUS_BASES_APPLIED	deviceCustomDate2, deviceCustomDate2Label, cnt, deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTISPAM_BASES_APPLIED	deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTIPHISHING_BASES_APPLIED	deviceCustomDate1, deviceCustomDate1Label
LMS_EV_ANTIVIRUS_BASES_UPDATE_ERROR	reason
LMS_EV_ANTISPAM_BASES_UPDATE_ERROR	reason
LMS_EV_ANTIPHISHING_BASES_UPDATE_ERROR	reason

kaspersky

Классы событий группы ScanLogic

В теле CEF-сообщений классов событий группы ScanLogic допустимо использование ключей в соответствии с их семантикой (см. таблицу ниже).

Таблица 37. Допустимые значения полей классов событий группы ScanLogic

Класс событий	Ключ	Значение
Все классы группы ScanLogic	cs1	ID сообщения.
	cs1Label	Всегда имеет значение `MessageId`.
	src	IP-адрес сервера, от которого получено сообщение.
	act	Действие.
	fsize	Размер сообщения.
	suser	Отправитель сообщения.
	duser	Список получателей сообщения.
	reason	Причина возникновения события.
	cs2	Список правил.
	cs2Label	Всегда имеет значение `Rules`.
	outcome	Статус проверки.
	cs3	Список получателей сообщения с вредоносными объектами или другими объектами, которые могут быть использованы злоумышленниками (с действием Skip).
	cs3Label	Всегда имеет значение `UnsafeRecipients`.
	fname	Имя файла.
LMS_EV_SCAN_LOGIC_AS_STATUS LMS_EV_SCAN_LOGIC_AP_STATUS	cs4	Метод обнаружения.
	cs4Label	Всегда имеет значение `Method`.
LMS_EV_SCAN_LOGIC_MA_STATUS	cs4	Заключение SPF.
	cs4Label	Всегда имеет значение `SpfVerdict`.

Класс событий	Ключ	Значение
	cs5	Заключение DKIM.
	cs5Label	Всегда имеет значение `DkimVerdict`.
	cs6	Заключение DMARC.
	cs6Label	Всегда имеет значение `DmarcVerdict`.
LMS_EV_SCAN_LOGIC_KT_STATUS	suser	Имя учетной записи пользователя, который извлек сообщение из KATA-карантина.
	cs4	Причина пропуска сканирования.
	cs4Label	Всегда имеет значение `SkipReason`.
LMS_EV_SCAN_LOGIC_CF_STATUS	cs4	• `BannedFileFormat`; • `BannedFileName`; • `BannedFileSize`.
	cs4Label	Всегда имеет значение `BannedEntity`.
LMS_EV_SCAN_LOGIC_PART_RESULT	cn1	Количество объектов.
	cn1Label	Всегда имеет значение `ObjectsNumber`.
	cs2	Список правил.
	cs2Label	Всегда имеет значение `Rules`.
	cs3	Непроверенные файлы.
	cs3Label	Всегда имеет значение `AvExclude`.
	cs4	Имена угроз.
	cs4Label	Всегда имеет значение `Threats`.
	cs5	Имя заблокированного файла.
	cs5Label	Всегда имеет значение `BannedFileName`.
	cs6	Формат заблокированного файла.
	cs6Label	Всегда имеет значение `BannedFileFormat`.

В каждом классе событий группы ScanLogic допустимо присутствие только релевантных ему ключей (см. таблицу ниже).

Таблица 38. Релевантные ключи для классов событий группы ScanLogic

Класс событий	Релевантные ключи
LMS_EV_SCAN_LOGIC_ALL_NOT_PROCESSED	cs1, cs1Label, src, act, fsize, suser, duser
LMS_EV_SCAN_LOGIC_AS_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label
LMS_EV_SCAN_LOGIC_AV_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, outcome
LMS_EV_SCAN_LOGIC_AP_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, outcome
LMS_EV_SCAN_LOGIC_KT_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, suser, outcome
LMS_EV_SCAN_LOGIC_MA_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, outcome
LMS_EV_SCAN_LOGIC_CF_STATUS	cs1, cs1Label, src, act, fsize, suser, duser, cs2, cs2Label, cs3, cs3Label, reason, cs4, cs4Label, outcome
LMS_EV_SCAN_LOGIC_PART_RESULT	cs1, cs1Label, cn1, cn1Label, fname, act, reason, cs2, cs2Label, cs3, cs3Label, cs4, cs4Label, cs5, cs5Label, cs6, cs6Label, outcome
LMS_EV_SCAN_LOGIC_MESSAGE_BACKUP	cs1, cs1Label, src, act, fsize, suser, duser, reason, cs2, cs2Label

Если в событии LMS_EV_SCAN_LOGIC_PART_RESULT в поле mime part указан статус `avStatus=Infected` или `avStatus=Disinfected`, то в качестве значения ключа `cn1` указывается список `disinfectedObjects` или `deletedObjects` при наличии одного из них. Если оба списка непустые, то ключи `cn1` и `cn1Label` будут добавлены дважды.

kaspersky

Антивирусная проверка модулем kavscanner

В состав Kaspersky Secure Mail Gateway входит модуль kavscanner, выполняющий антивирусную проверку файлов.

В этом разделе

Конфигурационный файл

В поставку Kaspersky Secure Mail Gateway входит конфигурационный файл модуля kavscanner **kavscanner_defaults.conf**, содержащий параметры работы модуля kavscanner. Конфигурационный файл находится в директории `/etc/opt/kaspersky/ksmg/kavscanner_defaults.conf`.

В этом разделе

Секция [locale]

Секция [locale] содержит параметры, определяющие форматы даты и времени:

- **DateFormat=%d-%m-%y**. Формат представления даты согласно strftime.

  Вы можете изменить формат представления даты, например, на: **%y/%m/%d или %m/%d/%y**.

- **TimeFormat=%H:%M:%S**. Формат представления времени согласно strftime.

  Вы можете изменить формат представления времени на двенадцатичасовой (am, pm): **%I:%M:%S %P**.

Секция [scanner.options]

Секция [scanner.options] содержит параметры проверки файловых систем сервера:

- **SelfExtArchives=yes**. Режим проверки самораспаковывающихся архивов.

  Для отключения режима присвойте параметру значение **no**.

  Если включен режим проверки архивов (**Archives=yes**), самораспаковывающиеся архивы будут проверены, даже если параметру **SelfExtArchives** присвоено значение **no**.

- **ExcludeDirs=маска1:маска2:...:маскаN**. Маски каталогов, которые исключаются из проверки.

  По умолчанию проверяются все каталоги.

  Маски задаются в виде стандартных shell-масок.

- **MailBases=yes**. Режим проверки почтовых баз.

  Для отключения режима присвойте параметру значение **no**.

- **Archives=yes**. Режим проверки архивов.

  Для отключения режима присвойте параметру значение **no**.

- **Packed=yes**. Режим проверки запакованных файлов.

  Для отключения режима присвойте параметру значение **no**.

- **ExcludeMask=маска1:маска2:...:маскаN**. Маски файлов, которые исключаются из проверки.

  По умолчанию проверяются все файлы.

  Маски задаются в виде стандартных shell-масок.

- **MaxLoadAvg**. Максимальная загрузка процессора. В случае превышения данного значения компонент kavscanner прекращает работу.

- **LocalFS=false**. Режим проверки только локальной файловой системы.

  Для включения режима присвойте параметру значение **true**.

- **Cure=no**. Режим лечения инфицированных объектов.

  Для включения режима присвойте параметру значение **yes**.

- **MailPlain=yes**. Режим проверки почтовых сообщений в виде plain text.

  Для отключения режима присвойте параметру значение **no**.

- **Heuristic=yes**. Режим использования во время проверки эвристического анализатора кода.

  Для отключения режима присвойте параметру значение **no**.

- **Recursion=true**. Режим рекурсивного прохода каталогов при проверке на наличие вирусов.

  Для отключения режима присвойте параметру значение **false**.

- **FollowSymlinks**. Режим работы с символьными ссылками.

  Если параметру присвоено значение **true**, при проверке будут раскрываться ссылки, указывающие на директорию.

Секция [scanner.options.other]

Секция [scanner.options.other] содержит параметры проверки легальных программ, которые могут быть использованы злоумышленниками:

- **EnableOtherProgramsDetectiom=false**. Режим проверки легальных программ.

  Для включения режима присвойте параметру значение **true**.

- **OtherProgramsAreThreats=false**. Результат проверки легальных программ.

  По умолчанию легальные программы не признаются угрозами. Чтобы утилита классифицировала легальные программы как угрозы, присвойте параметру значение **true**.

Секция [scanner.report]

Секция [scanner.report] содержит параметры формирования отчета о результатах работы компонента kavscanner:

- **Append=yes**. Режим добавления новых сообщений в файл отчета.

  Для отключения режима присвойте параметру значение **no**.

- **ShowContainerResultOnly=false**. Режим отображения в отчете результатов проверки архива в кратком формате.

  Для отображения краткого отчета присвойте параметру значение **true**.

- **ShowOK=false**. Режим вывода в отчет сообщений о незараженных файлах.

  Для включения режима присвойте параметру значение **true**.

- **ReportLevel=4**. Уровень детализации отчета.

- **ShowObjectResultOnly=false**. Режим отображения в отчете результатов проверки простого объекта в кратком формате.

  Для отображения результатов проверки в кратком формате присвойте параметру значение **no**.

- **ReportFileName**. Имя файла отчета, в котором фиксируются результаты работы компонента.

  Если параметру задано значение **syslog**, информация будет записана в системный журнал под категорией daemon.

Секция [scanner.container]

Секция [scanner.container] включает параметры, определяющие действия над архивами при антивирусной защите файловых систем сервера:

- **OnCorrupted=действие**. Действия в случае обнаружения поврежденного контейнера.
- **OnInfected=действие**. Действия в случае обнаружения зараженного объекта в контейнере. Если включен режим лечения зараженных файлов, то данное действие применяется к контейнерам, вылечить которые не удалось, и выполняется после всех действий с объектами контейнера.
- **OnWarning=действие**. Действия в случае обнаружения внутри контейнера объекта, код которого сходен с кодом известного вируса.
- **OnCured=действие**. Действия в случае обнаружения внутри контейнера зараженного объекта, который был успешно вылечен.
- **OnProtected=действие**. Действия в случае обнаружения внутри контейнера объекта, зашифрованного паролем. Такие объекты проверить невозможно.
- **OnError=действие**. Действия в случае возникновения ошибки при проверке контейнера.

Секция [scanner.object]

Секция [scanner.object] содержит параметры, определяющие действия над простыми объектами того или иного типа при антивирусной защите файловых серверов:

- **OnCorrupted=действие**. Действия в случае обнаружения поврежденного файла.
- **OnInfected=действие**. Действия в случае обнаружения зараженного файла.

  Если включен режим лечения зараженных файлов, то данное действие применяется к объектам, которые не удалось вылечить.
- **OnWarning=действие**. Действия в случае обнаружения файла, код которого сходен с кодом известного вируса.
- **OnCured=действие**. Действия в случае обнаружения и успешного лечения зараженного объекта.
- **OnProtected=действие**. Действия в случае обнаружения объекта, зашифрованного паролем. Такие объекты проверить невозможно.
- **OnError=действие**. Действия в случае возникновения ошибки при проверке объекта.

Секция [scanner.display]

Секция [scanner.display] содержит параметры вывода отчета на консоль управления:

- **ShowContainerResultOnly=false**. Режим отображения на консоли управления результатов проверки архива в кратком формате.

  Для отображения результатов проверки в кратком формате присвойте параметру значение **true**.
- **ShowObjectResultOnly=false**. Режим отображения на консоли управления результатов проверки простого объекта в кратком формате.

  Для отображения краткого отчета присвойте параметру значение **true**.
- **ShowOK=true**. Режим вывода на консоль управления сообщений о незараженных файлах.

  Для отключения режима присвойте параметру значение **false**.

- **ShowProgress=true**. Режим отражения на консоли управления текущей работы компонента (процесс загрузки антивирусных баз, информация о проверке текущего файла).

  Для отключения режима присвойте параметру значение **false**.

Секция [scanner.path]

Секция [scanner.path] содержит параметр, определяющий путь к файлам, без которых модуль kavscanner не будет функционировать:

BackupPath= путь. Полный путь к каталогу хранения резервных копий объектов, проверяемых компонентом.

Ключи командной строки

Параметры конфигурационного файла можно переопределить из командной строки при запуске программы с помощью ключей командной строки.

Опции помощи:

- **–h**. Вывести на консоль справочную информацию о компоненте kavscanner;
- **–v**. Показать версию программы.

Опции конфигурации:

- **–c (–C) <путь_к_файлу>**. Использовать альтернативный конфигурационный файл <путь_к_файлу>.
- **–f**. Игнорировать испорченную подпись компонента kavscanner и пытаться вылечить компонент.

Опции проверки:

- **–e <опция>**. Изменить опцию проверки, используемую по умолчанию. В качестве <опция> могут быть использованы следующие режимы:
  - **P/p**. Включить/выключить проверку упакованных файлов.
  - **A/a**. Включить/выключить проверку архивов.
  - **S/s**. Включить/выключить проверку самораспаковывающихся архивов.
  - **B/b**. Включить/выключить проверку почтовых баз.
  - **M/m**. Включить/выключить проверку сообщений в виде plain text.
  - **E/e**. Включить/выключить эвристический анализатор кода.
- **–R/r**. Включить/выключить рекурсивную проверку.
- **-S/s**. Включить/выключить режим раскрытия символьных ссылок.
- **–l**. Проверять только локальные файловые системы.

Опции формирования отчета:

- **–q**. Не выводить на консоль сообщения.
- **–o <имя>**. Задать имя файла, в который будет выводиться отчет о работе компонента. Если имя файла не задано, то отчет формироваться не будет. Помимо файла, информация о работе компонента будет выведена на консоль управления. Для вывода информации в системный журнал задайте syslog в качестве значения параметра <имя>.

- **–j<число>**. Задать уровень детализации отчета по объему содержащейся в нем информации. В качестве <опция> можно использовать следующие уровни детализации:
  - **1**. Сообщения об ошибках.
  - **2**. Информационные сообщения.
  - **3**. Сообщения о проверке.
  - **10**. Уровень отладки.
- **–x<опция>**. Задать уровень детализации отчета о проверке, выводимого на консоль управления. В качестве <опция> можно использовать следующие уровни детализации:
  - **O/o**. Краткий/расширенный формат сообщений о проверке простого объекта.
  - **C/c**. Краткий/расширенный формат сообщений о проверке архива.
  - **N/n**. Включить/выключить вывод на экран сообщений о незараженных файлах.
  - **P/p**. Включить/выключить вывод на консоль управления информации о текущей работе компонента.
- **–m<опция>**. Задать уровень детализации отчета о проверке, выводимого в файл отчета. В качестве <опция> могут быть использованы:
  - **O/o**. Краткий/расширенный формат сообщений о проверке простого объекта.
  - **C/c**. Краткий/расширенный формат сообщений о проверке архива.
  - **N/n**. Включить/выключить вывод в файл отчета сообщений о незараженных файлах.

Опции файлов:

- **–p<опция> <имя_файла>**. Сохранить список объектов в заданный файл, сохранять каждый объект с полным путем с новой строки. В качестве <опция> могут быть использованы:
  - **i**. Сохранить в файл <имя_файла> список инфицированных объектов.
  - **c**. Сохранить в файл <имя_файла> список поврежденных объектов.
  - **w**. Сохранить в файл <имя_файла> список объектов, код которых похож на код известных вирусов.
- **–@ <filelist.lst>**. Проверить объекты, путь к которым приведен в файле <filelist.lst>.

Опции обработки файлов (определение данных ключей в командной строке отменяет выполнение действий, заданных в конфигурационном файле):

- **–i0**. Только проверять на присутствие вирусов.
- **–i1**. Лечить зараженные объекты. Если лечение невозможно – пропустить.
- **–i2**. Лечить зараженные объекты. Если лечение невозможно, и объект является простым – удалить; зараженный объект из контейнера не удалять.
- **–i3**. Лечить зараженные объекты. Если лечение невозможно, и объект является простым – удалить; если зараженный объект находится в контейнере – удалить контейнер целиком.
- **–i4**. Удалить зараженные объекты и контейнеры.

kaspersky

Коды возврата

В процессе работы компонент kavscanner может возвращать следующие коды:

- **0**. Вирусы не найдены.
- **5**. Все зараженные объекты были вылечены.
- **10**. Обнаружены архивы, защищенные паролем.
- **15**. Обнаружены поврежденные файлы.
- **20**. Обнаружены возможно зараженные файлы.
- **21**. Обнаружены файлы, код которых похож на код известных вирусов.
- **25**. Обнаружены зараженные файлы.
- **30**. При проверке файлов возникла системная ошибка.
- **50**. Невозможно загрузить антивирусные базы (путь, указанный в конфигурационном файле, не найден).
- **55**. Антивирусные базы повреждены.
- **60**. Дата антивирусных баз выходит за пределы срока действия ключа.
- **64**. Лицензионная информация отсутствует, либо не найдено ни одного ключа по пути, указанному в конфигурационном файле.
- **65**. Невозможно загрузить конфигурационный файл.
- **66**. Неверная опция конфигурационного файла.
- **70**. Компонент kavscanner поврежден.
- **75**. Компонент kavscanner поврежден и не может быть вылечен.

Запуск и проверка работы модуля

► *Чтобы запустить модуль kavscanner и проверить его работу, выполните следующие действия:*

4. Войдите в режим Technical Support Mode.
5. Отключите проверку доступа на чтение файлов для процесса scan-сервера. Введите команду:

   ```
   # setcap cap_dac_read_search+ep /opt/kaspersky/ksmg/libexec/scan_server
   ```

6. Перезагрузите службу klms. Введите команду:

   ```
   # service ksmg restart
   ```

7. Проверьте права доступа к директории. Введите команду:

   ```
   # ls -lahd /root/
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   dr-xr-x--- 5 root root 4.0K Oct  6 20:10 /root/
   ```

8. Проверьте наличие файла `eicar.com` в текущей директории. Введите команду:

   ```
   # ls -lah /root/eicar.com
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   -rw-r--r-- 1 root root 69 Dec 22 09:22 /root/eicar.com
   ```

9. Запустите модуль kavscanner, убедитесь, что модуль kavscanner проверил файл `eicar.com`, обнаружил, что файл заражен и удалил его из директории. Введите команду:

   ```
   # /opt/kaspersky/ksmg/bin/kavscanner -i4 eicar.com
   ```

   Результатом успешного выполнения команды будет, например:

   ```
   Kaspersky Anti-Virus On-Demand Scanner.
   The latest bases update 26-12-2021
   Config file: /etc/opt/kaspersky/ksmg/kavscanner_defaults.conf
   /root/eicar.com INFECTED EICAR-Test-File
   ```

10. Убедитесь, что зараженный файл `eicar.com` действительно удален. Введите команду:

    ```
    # ls -lah /root/eicar.com
    ```

    Результатом выполнения команды будет, например:

    ```
    ls: cannot access /root/eicar.com: No such file or directory
    ```

kaspersky

Проверка сохраненных сообщений модулем EML-scanner

В состав Kaspersky Secure Mail Gateway входит модуль EML-scanner, выполняющий проверку сохранённых сообщений электронной почты с расширением .eml.

Администратор имеет возможность указать следующие технологии проверки сообщения:

- Анти-Фишинг (`ap`);
- Антивирус (`av`);
- Анти-Спам (`as`);
- Проверка ссылок (`mlf`).

Проверка возможна только при наличии действующего лицензионного ключа, определяющего набор доступных технологий проверки (см. раздел "Режимы работы Kaspersky Secure Mail Gateway в соответствии с лицензией" на стр. 41).

По завершении модуль выводит на консоль результат проверки сообщения технологиями, указанными при запуске. Модуль не производит никаких действий с проверяемыми сообщениями.

В этом разделе

Ключи командной строки

При работе с модулем из командной строки доступны следующие ключи:

- **--help**. Вывести на консоль справочную информацию о компоненте eml_scanner.
- **--av**. Выполнить антивирусную проверку сообщения.
- **--as**. Выполнить проверку сообщения на спам.
- **--ap**. Выполнить проверку сообщения на фишинг.
- **--mlf**. Выполнить проверку сообщения на наличие вредоносных и рекламных ссылок, а также ссылок, связанных с легальными программами.
- **--f [--file] arg**. Путь к файлу сохраненного сообщения, который требуется проверить.
- **--envelope-from arg**. Адрес отправителя сообщения.
- **--envelope-to arg**. Список получателей сообщения.
- **--helo arg**. HELO-имя сервера.
- **--client arg**. Имя SMTP-клиента.
- **--ip arg (=127.0.0.1)**. IP-адрес хоста.

kaspersky

Коды возврата

В процессе работы модуль EML-scanner отображает в консоли код возврата. Если обнаружение выполнено несколькими технологиями, соблюдается следующий приоритет кодов возврата:

- **0**. Угрозы не найдены.
- **1**. Обнаружены зараженные или возможно зараженные файлы.
- **2**. Обнаружены вредоносные, рекламные или связанные с легальными программами ссылки.
- **3**. Обнаружен фишинг.
- **4**. Обнаружен спам, возможный спам или массовая рассылка.
- **10**. Ошибка инициализации модуля (неверный синтаксис команды, не найден файл по указанному пути и т.д.).
- **11**. Ошибка лицензирования хотя бы одной из технологий проверки.
- **12**. Ошибка во время проверки файла.

Запуск и проверка работы модуля

► *Чтобы запустить модуль EML-scanner и проверить его работу, выполните следующие действия:*

11. Войдите в режим Technical Support Mode.
12. Отключите проверку доступа на чтение файлов для процесса scan-сервера. Введите команду:

    ```
    # setcap cap_dac_read_search+ep /opt/kaspersky/ksmg/libexec/scan_server
    ```

13. Перезагрузите службу ksmg. Введите команду:

    ```
    # service ksmg restart
    ```

14. Проверьте права доступа к директории. Введите команду:

    ```
    # ls -lahd /root/
    ```

    Результатом успешного выполнения команды будет, например:

    ```
    dr-xr-x--- 5 root root 4.0K Oct  6 20:10 /root/
    ```

15. Сохраните сообщение с расширением .eml, содержащее файл `eicar.com`, в текущей директории.
16. Запустите модуль EML-scanner и убедитесь, что модуль проверил сообщение с файлом `eicar.com` и обнаружил, что файл заражен. Для этого выполните команду:

    ```
    # /opt/kaspersky/ksmg/libexec/klms_eml_scanner --av -f /root/<имя файла>.eml
    ```

kaspersky

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Secure Mail Gateway (see section "Источники информации о программе" on page 16), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Secure Mail Gateway.

Kaspersky предоставляет поддержку Kaspersky Secure Mail Gateway в течение жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- позвонить в Службу технической поддержки по телефону (https://support.kaspersky.ru/b2c) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Вы можете найти информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки на веб-сайте Службы технической поддержки "Лаборатории Касперского" (https://support.kaspersky.ru/b2c).

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

kaspersky

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

Получение информации для Службы технической поддержки

После того как вы проинформируете специалистов Службы технической поддержки "Лаборатории Касперского" о возникшей проблеме, они могут попросить вас предоставить отладочную информацию, которая содержит в себе файлы трассировки и дополнительную информацию об операционной системе, запущенных процессах на сервере и другую диагностическую информацию. Файлы трассировки позволяют отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка. Вы можете выбрать, какие события будут записаны в файлы трассировки (ошибки или информационные сообщения). Все файлы трассировки и дополнительная отладочная информация помещаются в архив, который вы сможете передать в Службу технической поддержки.

Файлы трассировки могут содержать данные о вашей организации, которые вы считаете конфиденциальными. Необходимо согласовать состав отправляемого архива (см. раздел "О предоставлении данных" на стр. 25) со Службой безопасности вашей организации. Перед отправкой журнала трассировки удалите из него все данные, которые вы считаете конфиденциальными.

kaspersky

Отладочная информация о работе программы записывается в соответствии с заданным уровнем трассировки (см. раздел "Изменение уровня трассировки" на стр. 329).

Все операции с диагностической информацией доступны при наличии права **Получать диагностическую информацию**.

В этом разделе

Запуск трассировки

► *Чтобы запустить трассировку:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

   В рабочей области отобразится таблица узлов кластера с информацией о предыдущих запусках трассировки.
3. В таблице выберите узел, для которого вы хотите получить диагностическую информацию.

   Откроется окно **Просмотреть архивы**.
4. В правом нижнем углу нажмите на кнопку **Запустить**.

Трассировка будет запущена. В результате выполнения задачи отобразится информация о полученном архиве с диагностической информацией. Вы можете скачать (см. раздел "Скачивание файла трассировки" на стр. 330) или удалить (см. раздел "Удаление файла трассировки" на стр. 330) полученный архив.

Изменение уровня трассировки

Изменение уровня трассировки сохраняется в конфигурации программы и не влияет на уже созданные файлы трассировки.

► *Чтобы изменить уровень трассировки:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.
3. По ссылке Уровень диагностики в верхней части рабочей области откройте окно **Уровень диагностики**.
4. Выберите один из следующих вариантов:

- **Ошибки**.
- **Отладка**.

  Этот уровень трассировки значительно повышает требования к подсистеме хранения данных и снижает производительность программы. Используйте уровень отладки только если Служба технической поддержки "Лаборатории Касперского" просит предоставить файлы трассировки такого типа.

По умолчанию установлено значение **Ошибки**.

5. Нажмите на кнопку **Сохранить**.

Уровень трассировки будет изменен. Новые файлы трассировки будут создаваться в соответствии с выбранным уровнем.

Скачивание файла трассировки

► *Чтобы скачать файл трассировки:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

   В рабочей области отобразится таблица узлов кластера с информацией о предыдущих запусках трассировки.
3. В таблице выберите узел, для которого вы хотите скачать файл трассировки.

   Откроется окно **Просмотреть архивы**.
4. В строке с нужным файлом нажмите на значок справа от названия файла.

Архив с файлом будет сохранен на вашем компьютере в папке загрузки браузера.

Удаление файла трассировки

► *Чтобы удалить файл трассировки:*

1. В окне веб-интерфейса программы выберите раздел **Узлы**.
2. По ссылке **Получить диагностическую информацию** в верхней части рабочей области откройте окно **Диагностическая информация для Службы технической поддержки**.

   В рабочей области отобразится таблица узлов кластера с информацией о предыдущих запусках трассировки.
3. В таблице выберите узел, для которого вы хотите удалить файл трассировки.

   Откроется окно **Просмотреть архивы**.
4. В строке с нужным файлом нажмите на значок справа от названия файла.
5. В окне подтверждения нажмите на кнопку **ОК**.

Архив с файлом будет удален из списка.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программы, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию программы, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

Действия после сбоя или неустранимой ошибки в работе программы

Для предотвращения потери данных в случае возникновения сбоя или ошибки в работе программы рекомендуется периодически сохранять значения параметров, копию хранилища, информацию о системе, а также журнал аудита.

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Обращение в Службу технической поддержки" на стр. 327).

kaspersky

Глоссарий

A

Advanced persistent threat (APT)

Сложная целевая атака на IT-инфраструктуру организации с одновременным использованием различных методов проникновения в сеть, закрепления в сети и получения регулярного доступа к конфиденциальным данным.

D

DKIM-проверка подлинности отправителей сообщений

Проверка цифровой подписи к сообщениям.

DMARC-проверка подлинности отправителей сообщений

Проверка, определяющая политику и действия над сообщениями по результатам SPF- и DKIM-проверок подлинности отправителей сообщений.

DNSBL

DNS blacklist или DNS blocklist. Пользовательский список DNSBL-серверов, используемый для повышения уровня обнаружения спама. На DNSBL-серверах хранятся списки IP-адресов, которые были ранее замечены в рассылке спама и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам.

K

Kaspersky Anti Targeted Attack Platform

Решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как *атаки "нулевого дня"*, *целевые атаки* и сложные целевые атаки *advanced persistent threats* (далее также "*APT*").

Kaspersky Private Security Network

Решение, позволяющее пользователям антивирусных программ "Лаборатории Касперского" получать доступ к данным Kaspersky Security Network, не отправляя информацию на серверы Kaspersky Security Network "Лаборатории Касперского" со своей стороны.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

kaspersky

L

LDAP

Lightweight Directory Access Protocol – облегченный клиент-серверный протокол доступа к службам каталогов.

S

SNMP-агент

Программный модуль сетевого управления Kaspersky Secure Mail Gateway, отслеживает информацию о работе программы.

SNMP-ловушка

Уведомление о событиях работы программы, отправляемое SNMP-агентом.

SPF-проверка подлинности отправителей сообщений

Сопоставление IP-адресов отправителей сообщений со списком возможных источников сообщений, созданным администратором почтового сервера.

SURBL

Spam URI Realtime Blocklists. Пользовательский список SURBL-серверов, используемый для повышения уровня обнаружения спама. На SURBL-серверах хранятся списки веб-адресов, которые были ранее замечены в теме или в теле сообщений, расцененных как спам и которым модуль Анти-Спам присваивает спам-рейтинг и один из статусов проверки сообщений на спам.

A

Антивирус

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения вирусов в сообщениях электронной почты и вложениях в сообщения электронной почты.

Анти-Спам

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения сообщений, которые классифицируются как спам.

Анти-Фишинг

Компонент Kaspersky Secure Mail Gateway, предназначенный для обнаружения сообщений, которые классифицируются как фишинг.

Атака "нулевого дня"

Атака на IT-инфраструктуру организации, использующая уязвимости "нулевого дня" в программном обеспечении, которые становятся известны злоумышленникам до момента выпуска производителем программного обеспечения обновления, содержащего исправления.

В

Виртуальная машина

Полностью изолированная программная система, которая, исполняя машинно-независимый или машинный код процессора, способна имитировать операционную систему, приложения или устройства (например, компьютер).

Вредоносные ссылки

Веб-адреса, которые ведут на вредоносные ресурсы, то есть ресурсы, занимающиеся распространением вредоносного программного обеспечения.

К

Контентная фильтрация

Фильтрация сообщений электронной почты по размеру сообщения, маскам имен вложенных файлов и форматам вложенных файлов. По результатам контентной фильтрации можно ограничить пересылку сообщений почтовым сервером.

П

Почтовое уведомление

Сообщение электронной почты с описанием события программы или события проверки сообщений, которое Kaspersky Secure Mail Gateway отправляет на заданные адреса электронной почты.

Р

Репутационная фильтрация

Облачная служба, использующая технологии определения репутации сообщений. Информация о появлении новых видов спама в облачной службе появляется раньше, чем в базах модуля Анти-Спам, что дает возможность повысить скорость и точность обнаружения признаков спама в сообщении.

С

Служба каталогов

Программный комплекс, позволяющий хранить в одном месте информацию о сетевых ресурсах (например, о пользователях) и обеспечивающий централизованное управление ими.

Спам

Несанкционированная массовая рассылка сообщений электронной почты, чаще всего рекламного характера.

У

Уязвимость "нулевого дня"

Уязвимость в программном обеспечении, обнаруженная злоумышленниками до момента выпуска производителем программного обеспечения обновления, содержащего исправленный код программы.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии.

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Х

Хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов. Резервные копии создаются перед лечением или удалением зараженных объектов.

Ц

Целевая атака

Атака, направленная на конкретного человека или организацию. В отличие от массовых атак компьютерными вирусами, направленных на заражение максимального количества компьютеров, целевые атаки могут быть направлены на заражение сети определенной организации или даже одного сервера в IT-инфраструктуре организации. Для каждой целевой атаки может быть написана специальная троянская программа.

Э

Эвристический анализ

Технология обнаружения угроз, которые невозможно определить с помощью текущей версии баз программ "Лаборатории Касперского". Позволяет находить файлы, которые могут содержать неизвестный вирус или новую модификацию известного вируса.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

z/VM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Google Chrome – товарный знак Google, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Hyper-V, Internet Explorer, Windows и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Oracle – зарегистрированный товарный знак Oracle Corporation и/или ее аффилированных компаний.

Parallels Desktop является зарегистрированным товарным знаком Parallels International GmbH в США и/или других странах.

QT – товарный знак или зарегистрированный товарный знак The Qt Company Ltd.

CentOS – товарный знак компании Red Hat, Inc.

VMware, VMware ESXiV, Mware Server, VMware vSphere и VMware Workstation – товарные знаки VMware, Inc. или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

kaspersky

Предметный указатель

A

D

K

L

S

T

В

kaspersky

Д

Л

М

О

П

Х

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 39. Таблица соответствия терминов в документации и ФСТЭК

Термин в документации	Термин в требованиях ФСТЭК
Программа	Продукт, объект оценки, программное изделие
Вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
Антивирусные базы	Базы данных признаков компьютерных вирусов (БД ПКВ)
Антивирусная проверка	Поиск КВ
Администратор веб-интерфейса	Администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

Приложение. Значения параметров программы в сертифицированном режиме

Этот раздел содержит перечень параметров программы, влияющих на сертифицированный режим работы программы. В таблице ниже приведены значения этих параметров в сертифицированном режиме работы программы.

Если вы меняете какие-либо из перечисленных значений параметров с их значений в сертифицированном режиме работы программы на другие значения, вы выводите программу из сертифицированного режима работы.

Таблица 40. Параметры и их значения при работе программы в сертифицированном режиме

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Параметры → Общие → Защита	**Внешние службы**	**Использовать SPF-проверку**	**Включено**
		Использовать DKIM-проверку	
		Использовать DMARC-проверку	
	Антивирус	**Использовать Антивирус**	**Включено**
		Использовать эвристический анализ	
	Анти-Спам	**Использовать Анти-Спам**	**Включено**
		Использовать Анти-Спам карантин	
	Анти-Фишинг	**Использовать Анти-Фишинг**	**Включено**
	Контентная фильтрация	**Использовать Контентную фильтрацию**	**Включено**
Параметры → Внешние службы	**KSN/KPSN → Параметры KSN/KPSN**	**Использование KSN/KPSN**	**KPSN**
	Защита KATA → Параметры	**Отправлять на сервер KATA сообщения без обнаружений**	**Включено**, если настроена интеграция с Kaspersky Anti Targeted Attack Platform

Раздел / подраздел	Блок параметров	Название параметра	Значение параметра в сертифицированном режиме работы программы
Параметры правила **Default** в разделе **Правила**	**Общие**	**Режим**	**Использовать параметры модулей проверки**
	Анти-Спам		**Включено**
	Антивирус	**Антивирус**	**Включено**
		Если обнаружен зараженный объект	**Вылечить**
		Если обнаружены ошибки проверки модулем Антивирус	**Пропустить**
		Если обнаружен зашифрованный объект	
		Если обнаружен макрос	**Обрабатывать вложения с макросами**
		Если обнаружен макрос → Действие	**Удалить вложение**
	Защита KATA		**Включено**, если настроена интеграция с Kaspersky Anti Targeted Attack Platform
	Анти-Фишинг		**Включено**
	Контентная фильтрация		**Включено**
	Уведомления	Все параметры раздела	**Включено**, если настроено оповещение администратора безопасности по электронной почте об обнаруженных КВ
	Проверка подлинности		**Включено**